Supplemento ordinario alla “Gazzetta Ufficiale,, n. 261 del 9 novembre 2007 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b
Legge 23-12-1996, n. 662 - Filiale di Roma

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Venerdì, 9 novembre 2007** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00186 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00198 ROMA - CENTRALINO 06 85081

N. 229

MINISTERO DELL'INTERNO

DECRETO 8 novembre 2007.

Regole tecniche della Carta d'identità elettronica.

SOMMARIO

MINISTERO DELL'INTERNO

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELL'INTERNO

DECRETO 8 novembre 2007.

Regole tecniche della Carta d'identità elettronica.

IL MINISTRO DELL'INTERNO

DI CONCERTO CON

IL MINISTRO
PER LE RIFORME E LE INNOVAZIONI
NELLA PUBBLICA AMMINISTRAZIONE

E

IL MINISTRO
DELL'ECONOMIA E DELLE FINANZE

Visto l'art. 2 della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191;

Visto il regio decreto 18 giugno 1931, n. 773, ed il regio decreto 6 maggio 1940, n. 635;

Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;

Vista la legge 9 ottobre 2002, n. 222;

Visti gli articoli 64, 65 e in particolare l'art. 66, comma 6, del decreto legislativo 7 marzo 2005, 82, e successive modificazioni, recante Codice dell'Amministrazione Digitale»;

Considerato che la legge 31 marzo 2005, n. 43 ha disposto che dal 1° gennaio 2006 la carta d'identità su supporto cartaceo venga sostituita, all'atto della richiesta del primo rilascio o del rinnovo del documento, dalla carta d'identità elettronica;

Ravvisata, pertanto, la necessità e l'urgenza di aggiornare, sostituendolo con il presente decreto interministeriale che nella sua attività applicativa riguarda unicamente regole tecniche e di sicurezza relative a tecnologie e materiali, nonché le relative modalità di impiego, il decreto del Ministro dell'interno in data 19 luglio 2000, modificato con decreto ministeriale 14 maggio 2003, con decreto ministeriale 6 novembre 2003 e con decreto ministeriale 2 agosto 2005, recante regole tecniche e di sicurezza relative alla carta d'identità e al documento di identità elettronici, in attuazione delle disposizioni contenute nell'art. 7-*vicies ter* della legge n. 43 del 2005;

Tenuto conto delle indicazioni e delle proposte presentate dal Gruppo interministeriale di lavoro incaricato di collaborare alla realizzazione della fase di consolidamento e razionalizzazione della sperimentazione della carta d'identità elettronica, istituito con decreto ministeriale 25 gennaio 2002;

Tenuto conto delle direttive dell'Unione europea in merito all'interoperabilità tra documenti elettronici;

Vista la Direttiva 98/34/CE del Parlamento Europeo e del Consiglio, del 22 giugno 1998, modificata dalla Direttiva 98/48/CE del Parlamento Europeo e del Consiglio, del 20 luglio 1998, attuata dalla legge 21 giugno 1986, n. 317, modificata dal decreto legislativo 23 novembre 2000, n. 427;

Sentito il Garante per la protezione dei dati personali, che ha espresso parere favorevole in data 2 agosto;

D'intesa con la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281, espressa nella seduta del 20 settembre 2007.

Decreta:

CAPO I

PRINCIPI GENERALI

Art. 1.

Definizioni

1. Ai sensi del presente decreto si intende:

a) per «D.P.C.M.»: il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437;

a)-bis per «CIE»: la carta d'identità elettronica, ovvero il documento d'identità di cui all'art. 1, comma 1, lettera *c)* del decreto legislativo 7 marzo 2005, n. 82;

b) per «documento»: la carta d'identità elettronica e/o il documento d'identità elettronico di cui all'art. 2 del decreto del Presidente del Consiglio dei Ministri costituito dall'insieme del supporto fisico e dei supporti informatici;

b)-bis per «C.N.S.D.»: il Centro nazionale dei servizi demografici costituito con il decreto ministeriale 23 aprile 2002;

c) per «S.S.C.E.»: il sistema di servizi del C.N.S.D. per il circuito di emissione dei documenti;

c)-bis per «I.N.A.»: l'Indice nazionale delle anagrafi istituito con legge 28 febbraio 2001, n. 26;

c)-ter per «Backbone»: il backbone di sicurezza e certificazione per l'accesso ai servizi del C.N.S.D.;

c)-quater per «Sistema di sicurezza»: il sistema dei servizi di sicurezza del C.N.S.D.;

c)-quinquies per «Sistema di monitoraggio e allarme»: le funzioni di rilevazione degli allarmi di sicurezza e monitoraggio del funzionamento dei servizi del Sistema dei Servizi di sicurezza del C.N.S.D.;

d) per «S.A.I.A.»: il sistema predisposto dal Ministero dell'interno per l'accesso e l'interscambio anagrafico;

d)-bis per «porta applicativa»: la porta di accesso, attraverso il backbone, ai domini applicativi del C.N.S.D. utilizzata dal circuito di emissione CIE;

d)-ter per «porta di dominio»: la porta di accesso, realizzata secondo le specifiche SPC, ai domini applicativi del C.N.S.D. a disposizione delle amministrazioni (fruitori del servizio) che richiedono funzioni di cooperazione al C.N.S.D. (erogatore del servizio) tramite accordo di servizio;

e) per «Istituto»: l'Istituto Poligrafico e Zecca dello Stato;

f) per «dati riferiti alla persona»: i dati identificativi della persona di cui all'art. 1, comma 1, lettera *d)* e gli altri elementi di cui all'art. 3, comma 1, lettere da *b)* ad *h)*, del D.P.C.M.;

g) per «carta-servizi»: l'insieme dei dati di cui alla precedente lettera *f)* - ad esclusione della fotografia e della firma - e delle informazioni amministrative di cui all'art. 1, comma 1, lettera *e)* e dell'art. 3, comma 4, del D.P.C.M.;

h) per «codice cifrato»: i codici alfanumerici che identificano univocamente il microprocessore di ogni documento;

i) per «cartellino elettronico»: la trasposizione, in formato digitale e cifrata, del cartellino cartaceo di cui all'art. 290 del regio decreto 6 maggio 1940, n. 635;

j) per «P.I.N.»: il numero identificativo personale necessario alla fruizione dei servizi che ne richiedono l'utilizzo.

k) per «Comitato tecnico permanente»: il Comitato istituito con decreto dirigenziale del Ministero dell'interno in data 20 marzo 2003 con il compito di stabilire la perfetta corrispondenza dei supporti fisici prodotti dall'Istituto alle caratteristiche indicate nell'allegato B al presente decreto, nonchè l'idoneità tecnica e la compatibilità con il sistema di rete delle attrezzature da utilizzare per l'emissione della C.I.E.;

k)-bis per «Comitato tecnico-scientifico permanente»: il Comitato istituito ai sensi dell'art. 8-*bis* del presente decreto;

k)-ter per «Comitato di indirizzo e monitoraggio» il Comitato istituito ai sensi dell'art. 8-*ter* del presente decreto;

k)-quater per «Commissione di verifica e omologazione tecnica dei microprocessori» la Commissione istituita ai sensi dell'art. 8-*quater* del presente decreto;

l) per «sito»: il sito Web della carta d'identità elettronica accedibile all'indirizzo Internet www.interno.it;

m) per «certificato qualificato» il certificato elettronico di cui all'art. 1, comma 1, lettera *f)*, legge 7 marzo 2005, n. 82 e successive modificazioni;

n) per «finalità istituzionali»: utilizzo della CIE per nome e per conto del Ministero dell'interno;

o) per «MAE»: il Ministero degli affari esteri;

p) per «CAPA»: il Centro di allestimento e personalizzazione autonomo, realizzato presso il singolo Comune o anche in forma associata tra più Comuni, per i servizi di personalizzazione e stampa delle CIE da parte dei Comuni autonomi e Uffici consolari autonomi dotati di attrezzature di stampa autonome.

q) per «CAPS»: il Centro di allestimento e personalizzazione sussidiario, gestito direttamente e garantito dall'Istituto Poligrafico e Zecca dello Stato, che offre servizi di personalizzazione e stampa delle CIE alle strutture (Comuni, Uffici consolari) che non stampano in autonomia le CIE. Il CAPS può offrire, su richiesta, servizi di backup ai CAPA;

r) per «CA»: la struttura di Certification Authority del C.N.S.D.;

s) per «DM Sicurezza»: il decreto 2 agosto 2005 (nella *Gazzetta Ufficiale* n. 218 del 19 settembre 2005 - Supplemento ordinario n. 155) - Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE, in attuazione del comma 2, dell'art. 7-*vicies ter* della legge 31 marzo 2005, n. 43;

t) per «CSI»: il Centro Servizi di Informazione e logistica, gestito direttamente da IPZS, che coordina i processi di produzione dei supporti CIE. Gestisce inoltre i flussi di approvvigionamento dei supporti. Ospita un portale informativo per la gestione di informazioni logistiche (manutenzione apparati, tempi di consegna CIE, ...), realizzato in collaborazione con il Ministero dell'interno, a disposizione dei cittadini, dei Comuni emettitori e degli Uffici consolari. Garantisce, senza entrare nel merito del contenuto informativo della

comunicazione e senza conservare traccia alcuna dei dati, l'inoltro delle comunicazioni dal C.N.S.D. ai CAPS e viceversa;

u) per «postazione di emissione CIE»: apparato informatico dedicato al processo di emissione della CIE; possono essere postazioni per la sola fase di acquisizione dati (dedicate alla fase di front-office necessaria ad acquisire dal cittadino i dati riferiti alla sua persona), postazioni per la sola fase di allestimento e stampa (dedicate alla fase di scrittura del microprocessore e della banda ottica e al processo termografico di stampa della carta in bianco) o postazioni in grado di svolgere sia il processo di acquisizione dati che il processo di allestimento e stampa;

v) per «laboratorio di sicurezza del C.N.S.D.»: laboratorio scientifico del C.N.S.D. per lo studio e l'applicazione di standard e metodologie di sicurezza, microchip, algoritmi crittografici che si confronta a livello internazionale sugli standard tecnici con gli organismi competenti;

w) per «ICAO»: l'International Civil Aviation Organization;

x) per «autenticazione in rete»: l'autenticazione informatica tramite CIE di cui all'art. 1, comma 1 del decreto legislativo 7 marzo 2005, n. 82 finalizzata all'accesso ai servizi erogati in rete dalle pubbliche amministrazioni ai sensi dell'art. 64 del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni;

y) per «identificazione»: il riconoscimento, anche in rete, tramite CIE, dell'identità personale anagrafica del soggetto titolare della stessa ai sensi del Regolamento di esecuzione del testo unico delle leggi di P.S. (Regio decreto 18 giugno 1931, n. 773 e successive modificazioni) e dell'art. 66 del decreto legislativo 7 marzo 2005, n. 82.

Art. 2.

Funzioni dei Comuni

1) Le funzioni di pertinenza dei Comuni possono essere esercitate anche in forma associata.

2) I Comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato B al presente decreto, predispongono in piena autonomia i servizi locali.

Art. 3.

Modalità di connessione

1. Le amministrazioni e gli enti che, ai sensi della normativa vigente e del D.P.C.M., esercitano funzioni e svolgono compiti nell'ambito delle procedure di produzione, trasmissione, formazione, rilascio, rinnovo, aggiornamento e relativa verifica dei documenti, per l'espletamento di tali attività utilizzano in rete i servizi di sicurezza e di emissione del C.N.S.D. con le modalità di cui all'allegato B e, per quanto di loro competenza, devono provvedere all'aggiornamento dell'I.N.A.

Art. 4.

Misure di sicurezza

1. Ai fini della produzione, del rilascio, dell'aggiornamento e del rinnovo dei documenti, il trattamento dei dati, da parte delle amministrazioni e degli enti indicati dall'art. 3, comma 1, è effettuato nel rispetto del decreto legislativo 30 giugno 2003, n. 196, nonché delle ulteriori prescrizioni tecniche descritte nell'allegato B.

2. Le strutture coinvolte nelle diverse parti della filiera necessaria alla formazione e rilascio della CIE devono ottemperare, per la protezione delle comunicazioni e per le funzioni di propria competenza, alle prescrizioni di cui al decreto ministeriale Sicurezza. I CAPS, CAPA e gli Uffici consolari sono tenuti a definire, per le componenti di propria pertinenza, appositi Piani di sicurezza basati sul modello dei Piani di sicurezza comunali e del Piano di sicurezza del C.N.S.D. I piani di sicurezza dei CAPA realizzati in forma associata tra più Comuni devono essere predisposti congiuntamente da tutti i Comuni associati.

3. Il Ministero dell'interno e i Comuni sono titolari del trattamento di dati personali da essi rispettivamente effettuato.

Art. 5.

Servizi e modalità di autenticazione

1. Ai sensi dell'art. 3, comma 4, e dell'art. 7, comma 1, del decreto del Presidente del Consiglio dei Ministri, tutti i servizi che non implicano la memorizzazione dei dati sui documenti sono predisposti in piena autonomia dalle amministrazioni. Le modalità di autenticazione in rete per l'accesso ai servizi da parte del titolare del documento sono definite nell'allegato B.

2. Per i servizi che richiedono la memorizzazione di dati sui documenti è necessaria l'installazione degli stessi da parte del Comune e, qualora relativi a dati sensibili, la richiesta dell'interessato.

3. I servizi nazionali che richiedono la memorizzazione di dati sui documenti sono predisposti con le modalità e nel rispetto delle regole tecniche di cui all'allegato B.

4. Nell'attuazione dei servizi erogabili in rete non si procede in alcun caso al tracciamento e/o alla registrazione centralizzata presso il Ministero dell'interno di dati relativi all'utilizzo della carta per l'accesso ai servizi delle PP.AA., né dei servizi per cui è stata richiesta l'autenticazione.

CAPO II

Regole tecniche di base

Art. 5-*bis*.

Diffusione della documentazione

1. Tutta la documentazione ufficiale, normativa e tecnica, relativa alla carta d'identità elettronica è pubblicata sul sito.

Art. 6.

C.N.S.D.

1. Il Ministero dell'interno, con le modalità di cui all'allegato B, mette a disposizione delle Questure, dei Comuni, degli Uffici consolari e dell'Istituto l'infrastruttura organizzativa, informatica e di rete del C.N.S.D. e cura la realizzazione, la gestione e la manutenzione dei servizi di sicurezza e di emissione, nonché rende disponibili ai Comuni, agli Uffici consolari e ai centri di allestimento:

il software della porta applicativa di accesso al backbone, ai fini dell'utilizzazione dei servizi del C.N.S.D. da parte degli Enti emettitori;

il software di supporto all'uso in rete del documento, ai cittadini, ai Comuni e alle amministrazioni ed enti interessati;

il servizio di convalida I.N.A., attraverso backbone del C.N.S.D., direttamente dall'I.N.A.;

il servizio di validazione dei certificati digitali CIE, realizzato sullo standard OCSP (RFC 2560) per i sistemi che erogano servizi tramite il documento. L'accesso a tale servizio avviene tramite credenziali di sicurezza fornite dal Ministero dell'interno o dallo stesso riconosciute ed è reso disponibile direttamente dal Ministero dell'interno e attraverso strutture dallo stesso riconosciute ed è fruibile sia su SPC che su altre reti per gli enti non connessi a SPC. Nell'attuazione del servizio di validazione dei certificati digitali CIE non si procede in alcun caso al tracciamento e/o alla registrazione centralizzata presso il Ministero dell'interno di dati relativi all'utilizzo della carta per l'accesso ai servizi delle PP.AA., né dei servizi per cui è stata richiesta l'autenticazione;

i software di sicurezza e di emissione, finalizzati a garantire l'integrità, l'accessibilità e la riservatezza delle informazioni nelle fasi di compilazione, allestimento, stampa, rilascio, aggiornamento, rinnovo e verifica dei documenti ai Comuni e ai CAPA nonché finalizzati a garantire l'integrità e la sicurezza delle comunicazioni telematiche tra C.N.S.D., Comuni e centri di allestimento;

il servizio di notifica al CSI dell'operatività delle postazioni di allestimento e stampa dei CAPA;

pubblica il file system del documento.

Il Ministero dell'interno C.N.S.D. fornisce ai Comuni che acquisiscono in autonomia postazioni di emissione conformi alle specifiche tecniche pubblicate sul sito il necessario software di sicurezza ed emissione, nonché i relativi aggiornamenti.

In relazione alle banche dati del C.N.S.D. relative ai processi della CIE e quelle che vengono utilizzate anche in altri servizi del C.N.S.D. (quali l'I.N.A., l'A.I.R.E. e le banche dati per la validazione dei certificati digitali), il Sistema di sicurezza del C.N.S.D. fornisce le infrastrutture fisiche e logiche per assicurare sia l'effettiva separazione tra queste ultime banche dati e le banche dati del C.N.S.D. relative ai processi della CIE, sia l'impossibilità della loro consultabilità incrociata.

2. Ai sensi dell'art. 6, comma 1, del decreto del Presidente del Consiglio dei Ministri le questure, nei casi previsti dallo stesso articolo, procedono all'interdizione dell'operatività del documento secondo le modalità descritte nell'allegato B.

3. Le questure, ai sensi dell'art. 290 del regio decreto 6 maggio 1940, n. 635, conservano il cartellino elettronico, a cui accedono in via esclusiva, relativo ai documenti rilasciati dai Comuni della stessa provincia.

Art. 6-*bis*.

Utilizzo delle infrastrutture di servizio C.N.S.D. da parte di altri circuiti di emissione

1. Il supporto informatico del documento ne rende possibile l'utilizzo, con le modalità di cui all'allegato B, da parte di altri circuiti.

2. Le modalità operative di accesso e di utilizzo delle infrastrutture di servizio del C.N.S.D. devono di volta in volta essere concordate con il Ministero dell'interno.

I CAPS possono comunicare telematicamente con il C.N.S.D. per il tramite del CSI, fermo restando che al CSI non è consentito entrare nel merito del contenuto

informativo della comunicazione e conservare traccia alcuna dei dati: a tale scopo viene utilizzato il software di sicurezza di cui all'art. 6, comma 1.

Art. 7.

Supporto fisico

1. Il supporto fisico del documento è costituito da una carta plastica conforme alle norme ISO/IEC 7816-1, 7816-2 e ISO/ID-001 ed è integrato dai supporti informatici di cui all'art. 8.

2. Il supporto fisico è stampato con le tecniche tipiche della produzione di carte valori ed è dotato degli elementi fisici di sicurezza atti a consentire il controllo dell'autenticità del documento visivamente e mediante strumenti portatili e di laboratorio.

3. Il documento ha le caratteristiche grafiche di cui al modello approvato con il presente decreto e di cui all'allegato A.

Art. 8.

Supporti informatici

Il supporto fisico di cui all'art. 7 è dotato di una banda ottica per la memorizzazione, con modalità informatiche di sicurezza, dei dati riportati graficamente sul documento, nonché di un microprocessore per la memorizzazione della carta-servizi e per le operazioni connesse alle procedure di identificazione in rete del titolare del documento. Gli standard internazionali, le caratteristiche tecniche e l'architettura logica dei predetti supporti informatici sono conformi alle specifiche indicate nell'allegato B.

Art. 8-*bis*

Comitato tecnico-scientifico permanente

1. È istituito, con decreto del Ministro dell'interno, un Comitato tecnico-scientifico permanente, struttura tecnica del Ministero dell'interno di raccordo con i soggetti attuatori per la gestione operativa del progetto CIE e di supporto al Comitato di indirizzo e monitoraggio.

Il Comitato tecnico-scientifico permanente è composto da rappresentanti ed esperti nominati dal Ministero dell'interno e da esperti indicati da IPZS, CNIPA e da ANCI in rappresentanza dei Comuni. Alle sedute del Comitato partecipa inoltre il responsabile del coordinamento scientifico e progettuale dei progetti C.N.S.D. e CIE.

Al Comitato sono affidati anche i seguenti compiti:

definire e aggiornare costantemente gli standard tecnologici e le linee-guida per le attività correlate:

a) alla produzione e alla formazione dei supporti fisici;

b) alle caratteristiche della banda ottica;

c) alle caratteristiche del microprocessore e del file system;

d) alle caratteristiche dei dispositivi di acquisizione e stampa;

e) alla definizione delle modalità di utilizzo della CIE come strumento di firma digitale.

certificare le stampanti termografiche e i dispositivi di acquisizione dati biometrici, prima della loro distribuzione sul territorio.

2. Le determinazioni tecniche assunte dal Comitato sono pubblicate nel sito del Ministero dell'interno. Il Ministero dell'interno, nel caso si tratti di determinazioni relative alla definizione e all'aggiornamento di standard tecnologici o di linee guida le sottopone, prima della pubblicazione, al parere del Garante per la protezione dei dati personali.

3. Il Ministero dell'interno invia per conoscenza al Garante per la protezione dei dati personali tutte le determinazioni del Comitato relative a decisioni e pareri di monitoraggio, applicazione e valutazione dello stato di avanzamento del progetto CIE, che non ricadono tra quelle di cui al comma 2.

4. Il funzionamento e la partecipazione al predetto Comitato non comporterà oneri a carico dell'Amministrazione dello Stato.

Art. 8-*ter*

Comitato di indirizzo e monitoraggio

1. È istituito, con decreto del Ministro dell'interno, un Comitato di indirizzo e di monitoraggio.

I componenti del Comitato di indirizzo e di monitoraggio sono i seguenti:

un presidente designato dal Ministro dell'interno;

un rappresentante nominato dal Ministro dell'interno e un supplente;

un rappresentante nominato dal Ministro dell'economia e delle finanze e un supplente;

un rappresentante nominato dal Ministro per le riforme e le innovazioni nella pubblica amministrazione e un supplente;

un rappresentante nominato dal Ministro per gli affari regionali e le autonomie locali e un supplente;

un rappresentante nominato dalle Regioni e un supplente;

un rappresentante nominato dall'ANCI e un supplente.

Alle sedute del Comitato partecipa inoltre il responsabile del coordinamento scientifico e progettuale dei progetti C.N.S.D. e CIE.

Il Comitato di indirizzo e monitoraggio:

a) valuta lo stato di avanzamento del progetto CIE nei diversi ambiti e aspetti;

b) valuta le modalità di utilizzo della CIE come strumento di firma digitale;

c) controlla che i servizi erogati tramite CIE siano correttamente svolti, nel rispetto degli standard definiti dal Ministero dell'interno e dal Ministro per le riforme e le innovazioni nella Pubblica Amministrazione;

d) monitora le attività relative ai progetti per la diffusione dei servizi accessibili on line;

e) definisce i livelli di servizio delle componenti del progetto CIE e ne effettua il monitoraggio;

f) definisce e approva le linee guida sull'erogazione dei servizi on line e l'utilizzo della CIE;

g) controlla il rispetto degli standard di utilizzo della CIE.

2. Il Ministero dell'interno sottopone al parere del Garante per la protezione dei dati personali tutte le determinazioni del Comitato relative alla definizione e all'aggiornamento di standard tecnologici o di linee guida.

3. Il Ministero dell'interno invia per conoscenza al Garante per la protezione dei dati personali tutte le determinazioni del Comitato relative a decisioni e pareri di monitoraggio, applicazione e valutazione dello stato di avanzamento del progetto CIE, che non ricadono tra quelle di cui al comma 2.

4. Il funzionamento e la partecipazione al predetto Comitato non comporterà oneri a carico dell'Amministrazione dello Stato.

Art. 8-*quater*

Commissione di verifica e omologazione tecnica dei microprocessori

1. È istituita, con provvedimento del Ministero dell'interno, una Commissione di verifica e omologazione tecnica dei microprocessori.

I componenti della Commissione, presieduta da un funzionario del Ministero dell'interno, sono i seguenti:

un esperto del Ministero dell'interno e un supplente;

un esperto del Ministero dell'economia e delle finanze e un supplente;

un esperto del CNIPA in rappresentanza del Ministero per le riforme e le innovazioni nella pubblica amministrazione e un supplente;

un esperto dell'Istituto Poligrafico e Zecca dello Stato e un supplente.

Alle sedute della Commissione partecipa inoltre il responsabile del coordinamento scientifico e progettuale dei progetti C.N.S.D. e CIE.

2. Il Ministero dell'interno invia per conoscenza al Garante per la protezione dei dati personali tutte le determinazioni della Commissione relative a decisioni e pareri di monitoraggio, applicazione e valutazione dello stato di avanzamento del progetto CIE.

3. Il funzionamento e la partecipazione al predetto Comitato non comporterà oneri a carico dell'Amministrazione dello Stato.

Art. 9.

Inizializzazione del documento

1. L'Istituto, cui è riservata la produzione dei documenti a norma dell'art. 11 del presente decreto, provvede alla inizializzazione delle componenti fisiche ed informatiche del documento secondo le procedure di sicurezza descritte nell'allegato B. A seguito della inizializzazione il documento acquisisce la qualità di documento in bianco.

2. I supporti fisici prodotti nella prima fase di sperimentazione recano la numerazione da AA0000001 a AA0155940.

I supporti fisici prodotti nella seconda fase della sperimentazione sono numerati in progressione a partire da 0000001AA.

I supporti fisici prodotti a partire dall'entrata in vigore del presente decreto proseguiranno la numerazione della seconda fase della sperimentazione.

I numeri non attribuiti non possono essere riassegnati e verranno pubblicati con cadenza trimestrale nella *Gazzetta Ufficiale* con apposito decreto dirigenziale del Ministero dell'interno.

Art. 10.

Configurazione hardware e software per la formazione del documento

1. Ai fini della formazione dei documenti:

i Comuni e gli Uffici consolari utilizzano le specifiche configurazioni delle postazioni di acquisizione dati approvate dal Ministero dell'interno;

i Comuni, e gli Uffici consolari, dotati di CAPA utilizzano le specifiche configurazioni delle postazioni di acquisizione dati e delle postazioni di allestimento e stampa approvate dal Ministero dell'interno.

2. Ai fini della compilazione, rilascio, aggiornamento e rinnovo dei documenti, nonché delle comunicazioni con il C.N.S.D., i Comuni e gli Uffici consolari utilizzano il software di sicurezza di cui all'art. 6, comma 1.

3. Ai fini della riservatezza dei flussi di dati necessari per l'allestimento e della stampa dei documenti, nonché di tutte le altre comunicazioni con il C.N.S.D., i CAPS utilizzano, tenendo conto delle funzioni del CSI, il software di sicurezza di cui all'art. 6, comma 1.

4. L'Istituto, per le postazioni di emissione che fornisce direttamente, cura la fase di installazione del software, ricevuto dal Ministero dell'interno, sulle postazioni di acquisizione dati e sulle postazioni di allestimento e stampa destinate ai Comuni, Uffici consolari e CAPA, prima della loro attivazione.

CAPO III

NORME PROCEDIMENTALI

Art. 11.

Produzione del documento

1. La produzione del documento è riservata all'Istituto che vi provvede ottemperando alle norme che disciplinano la produzione delle carte valori e dei documenti di sicurezza della Repubblica italiana e agli standard internazionali di sicurezza previsti per l'emissione di carte di pagamento.

2. Nella fase di produzione a regime dei documenti elettronici di cui al presente decreto, l'Istituto, nell'ambito di proprio stabilimento, costituisce uno speciale settore con accesso limitato ai dipendenti addetti alle specifiche lavorazioni e sorvegliato dalle Forze di Polizia, dotato altresì delle sicurezze fisiche antieffrazione e dei sistemi di sorveglianza elettronici definiti di intesa con il Ministero dell'interno.

Art. 12.

Trasmissione del documento in bianco in periferia e sua custodia da parte del Comune

1. La trasmissione alle Prefetture dei documenti in bianco è effettuata dal Provveditorato Generale dello Stato, d'intesa con l'Istituto, in condizioni di sicurezza, mediante affidamento dei plichi a vettori specializzati nel trasporto di valori. Il Comune ritira presso la Prefettura i documenti in bianco ad esso assegnati. Nel caso di CAPA realizzato in forma associata il Comune responsabile del CAPA ritira presso la Prefettura sia i documenti in bianco ad esso assegnati che quelli assegnati agli altri Comuni associati nel CAPA, in base alle specifiche autorizzazioni ricevute dai singoli Comuni associati.

2. I Comuni dotati di proprio CAPA e i CAPA realizzati in forma associata adottano ogni idonea misura per la custodia dei documenti in bianco in condizioni di sicurezza in conformità al Piano di sicurezza di cui al «DM Sicurezza».

3. Il CAPS adotta ogni idonea misura per la custodia dei documenti in bianco in condizioni di sicurezza in conformità al Piano di sicurezza di cui al «DM Sicurezza».

Art. 13.

Procedura di sicurezza per la formazione e rilascio del documento

1. La formazione ed il rilascio del documento avvengono nel rispetto della seguente procedura di sicurezza:

a) il Comune, utilizzando le funzionalità del software di sicurezza di cui all'art. 10, comma 2, acquisisce al front-office i dati anagrafici e biometrici del richiedente;

b) il Comune, utilizzando le funzionalità del software di sicurezza di cui all'art. 10, comma 2, genera un messaggio informatico cifrato, costituito dai dati riferiti alla persona del richiedente e dai codici cifrati necessari all'identificazione del documento e lo invia in via telematica al Sistema di sicurezza del C.N.S.D.;

c) i dati, ad eccezione del codice fiscale e del numero identificativo del documento, vengono registrati cifrati dal Sistema di sicurezza del C.N.S.D.; l'accesso ai predetti dati in chiaro è consentito esclusivamente alla questura territorialmente competente e al Comune emettitore;

d) il Comune che si avvale di un proprio CAPA, ricevuta la necessaria abilitazione ad emettere il documento da parte della CA del C.N.S.D., riporta i dati identificativi della persona sul microprocessore e sulla banda ottica secondo le modalità indicate nell'allegato B ed effettua la stampa di tali dati sul supporto fisico. Il sistema di monitoraggio e allarme, mediante i suoi moduli periferici, rileva la stampa della carta e la segnala al sistema di contabilizzazione del C.N.S.D.;

e) il Comune, al front office, genera il P.I.N., lo stampa su carta chimica retinata in grado di garantire la riservatezza dell'informazione, segnala l'avvenuta emissione al Sistema di sicurezza del C.N.S.D. e lo consegna, insieme al documento, al titolare. Il sistema di monitoraggio e allarme, mediante i suoi moduli periferici, rileva l'emissione della carta e la segnala al sistema di contabilizzazione del C.N.S.D.. Il C.N.S.D. invia periodicamente tali dati di contabilizzazione all'Istituto, per alimentare il sistema di contabilizzazione del MEF;

f) Il Comune che procede in forma associata alla stampa della CIE, per la generazione del P.I.N. e la consegna della carta dovrà attendere di riceverla dal Comune responsabile del CAPA.

2. I Comuni che si avvalgono dei CAPS dell'Istituto ai fini della formazione del documento, utilizzano una configurazione hardware, per la componente di acquisizione dei dati e di rilascio del documento, conforme ad uno standard minimo corrispondente alle specifiche tecniche pubblicate sul sito e che rispetta i richiesti standard di sicurezza. Per i Comuni che si avvalgono dei CAPS, dopo che sono state effettuate le operazioni di cui al comma 1, punti *a)* e *b)*:

a) il Sistema di sicurezza del C.N.S.D., a fronte dei messaggi informatici cifrati di cui al comma 1, lettera *b)*, ancora privi del codice cifrato necessario per l'identificazione in rete del documento, predispone, a partire da tali messaggi informatici, un elenco classificato per Comune; segnala, a cadenze temporali prefissate, in via telematica al CAPS il numero di carte da stampare, e i relativi Comuni emettitori, desunti dall'elenco dei suddetti messaggi informatici;

b) il CAPS associa all'elenco ricevuto dal C.N.S.D. i codici cifrati necessari per l'identificazione in rete dei documenti e li invia al C.N.S.D. richiedendo alla CA del C.N.S.D. l'abilitazione all'allestimento dei documenti;

c) i dati, ad eccezione del codice fiscale e del numero identificativo del documento, vengono registrati cifrati dal Sistema di sicurezza del C.N.S.D.; l'accesso ai predetti dati in chiaro è consentito esclusivamente alla questura territorialmente competente e al Comune emettitore;

d) il CAPS, ricevuta la necessaria abilitazione ad emettere il documento da parte della CA del C.N.S.D., abilitazione firmata dal Sistema di sicurezza del C.N.S.D., riporta i dati identificativi della persona sul microprocessore e sulla banda ottica secondo le modalità indicate nell'allegato B ed effettua la stampa ditali dati sul supporto fisico;

e) I CAPS e i CAPA non conservano traccia dei dati utilizzati per la formazione del documento né forniscono a terzi tali dati, anche in modo parziale. Il CSI non conserva traccia dei dati ricevuti dal C.N.S.D. e trasmessi ai CAPS e viceversa. I CAPS generano un messaggio di conferma dell'avvenuta stampa e lo inviano al sistema di monitoraggio e allarme del C.N.S.D. per la contabilizzazione. I CAPS inviano al C.N.S.D. anche l'elenco delle carte la cui stampa è andata in errore. Il C.N.S.D. integrerà tali carte in un successivo elenco che seguirà le stesse modalità di lavorazione dal punto *a)* in avanti;

f) lo sportello di front-office del Comune, alla ricezione delle carte allestite dal CAPS o dal CAPA, genera il P.I.N., lo stampa su carta chimica retinata in grado di garantire la riservatezza dell'informazione, segnala l'avvenuta emissione al Sistema di sicurezza del C.N.S.D. e lo consegna, insieme al documento, al titolare. Il sistema di monitoraggio e allarme, mediante i suoi moduli periferici, rileva l'emissione della carta e la segnala al sistema di contabilizzazione del C.N.S.D.. Il C.N.S.D. invia periodicamente tali dati di contabilizzazione all'Istituto, per alimentare il sistema di contabilizzazione del MEF.

3. L'Istituto, che gestisce direttamente i CAPS, assicura, per quanto di competenza, a regime un livello di servizio che consente la disponibilità presso le Prefetture dei documenti formati entro il termine di (5) cinque giorni lavorativi successivi alla ricezione dell'abilitazione di cui al punto *d*, comma 2, e, comunque, non superiore ai quindici giorni lavorativi nel transitorio, dandone comunicazione ai competenti Uffici del Ministero dell'interno e di quello dell'economia e delle finanze. I Comuni ritirano presso le Prefetture, secondo le modalità indicate dal Ministero dell'interno, i documenti formati di loro competenza.

4. I Comuni che fanno ricorso a propri CAPA, assicurano, per quanto di competenza, livelli di servizio che consentano la disponibilità presso le proprie sedi comunali dei documenti formati entro il termine di due giorni lavorativi successivi alla ricezione dell'abilitazione di cui al comma 1, punto *d*.

5. I CAPS e i CAPA sono tenuti alla presentazione al Ministero dell'interno, coerentemente con le prescrizioni del «DM Sicurezza», dei piani di sicurezza per i processi di allestimento da essi svolti. L'approvazione di tali Piani di sicurezza da parte del Ministero dell'interno costituisce un prerequisito inderogabile per l'inizio delle loro attività nei confronti dei Comuni.

6. Gli Uffici consolari abilitati all'emissione della CIE sono tenuti alla presentazione al Ministero dell'interno, coerentemente con le prescrizione del «DM Sicurezza», dei Piani di sicurezza per i processi da essi svolti.

7. Il Sistema di sicurezza del C.N.S.D. fornisce ai CAPS e ai CAPA le quantità di sicurezza, generate dalla CA del C.N.S.D., necessarie alla loro autenticazione e alla sicurezza delle comunicazioni di rete con il C.N.S.D. stesso.

Art. 14.

Validità della CIE

1. L'eventuale estensione della durata della validità della CIE comporta l'aggiornamento delle regole tecniche di cui al presente decreto e dei relativi allegati.

Art. 15.

Emissione della CIE da parte dei Consolati

1. I Consolati italiani sono autorizzati all'emissione della CIE per i cittadini italiani che ne facessero richiesta presso gli Uffici Consolari stessi.

2. Con decreto interministeriale del Ministro dell'interno e del Ministro degli affari esteri verranno definite le modalità organizzative e tecniche di dettaglio per l'emissione della CIE da parte degli Uffici Consolari.

Art. 16.

Abrogazioni

1. Il presente decreto e relativi allegati sostituisce integralmente il decreto del Ministro dell'interno in data 19 luglio 2000, modificato con decreto ministeriale 14 maggio 2003, con decreto ministeriale 6 novembre 2004 e con decreto ministeriale 2 agosto 2005, recante regole tecniche e di sicurezza relative alla carta d'identità e al documento di identità elettronici.

Roma, 8 novembre 2007

Il Ministro dell'interno
AMATO

Il Ministro per le riforme e le innovazioni nella pubblica amministrazione
NICOLAIS

Il Ministro dell'economia e delle finanze
PADOA SCHIOPPA

ALLEGATO A

Caratteristiche grafiche del documento

ALLEGATO B

1 Introduzione

1.1 Bibliografia di riferimento e standard utilizzati

- Schema per il circuito di emissione della Carta di identita' elettronica, Roma 22 dicembre 1999 - AIPA/Associazioni dei fornitori - Gruppo di lavoro Carta d'identita' elettronica;
- Processo di autenticazione in rete. Roma 22 dicembre 1999 -
- AIPA/Associazioni dei fornitori - Gruppo di lavoro Carta d'identita' elettronica;
- Progetto del Centro nazionale servizio demografici - Roma, dicembre 2002 - Ministero Interno/Universita' di Roma Tor Vergata;
- ISO/IEC 9594-8:2001 per il formato dei certificati digitali, le estensioni e le policy;
- ISO/IEC 10118-3:1998 per la funzione di hash SHA-1;
- ISO/IEC 11694-1-2-3-4 Annex A e Annex B per la parte relativa alla banda ottica;
- ISO/IEC 7816-1-2-3-4-5-6-7-8-9 per la parte relativa alla smart card;
- PKCS11 per l'interfacciamento delle smart card;
- Allegato tecnico al Protocollo d'Intesa in data 13 maggio 2003 Governo - Produttori di microcircuiti.
- Comitato Tecnico Ristretto CIE, completamento dei lavori sul microchip della CIE, 21 aprile 2006.
- ICAO, documento 9303, parte 3
- Council of the European Union, "A" item note 15000/05, Hague Programme
- EU Regulation 2252/2004

1.2 Struttura della carta

La carta d'identità elettronica (**CIE**) è una carta ibrida, in grado di integrare nel supporto fisico sia una banda a memoria ottica che un microprocessore.

La banda ottica a lettura laser è utilizzata per la memorizzazione dei "dati" identificativi (D.M. Art. 1, comma 1, lettera f) ai fini della salvaguardia delle esigenze di pubblica sicurezza. L'elevata capacità di memoria disponibile, utilizzata per la memorizzazione di immagini o di informazioni di grosso volume, associata alla capacità elaborativa del microchip, può consentirne un utilizzo anche per la fruizione di servizi locali o nazionali.

Il microprocessore è utilizzato per assolvere le funzioni di "carta servizi" (DM Art. 1, comma 1, lettera g), per consentire l'autenticazione in rete e, quindi, l'erogazione di servizi telematici.

Le caratteristiche grafiche della CIE (D.M. art. 7, comma 3), unitamente al dettaglio delle informazioni presenti, sono riportate nell'allegato **A**.

2 Infrastruttura organizzativa (fa riferimento all'art.3 del D.M.)

Nel circuito di emissione intervengono gli enti nel seguito descritti:

Fornitori di microprocessori: *Aziende produttrici dei microprocessori.*
Provvedono alla fornitura dei microprocessori, durante la produzione memorizzano, in area leggibile e non riscrivibile, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di chip, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di microprocessori consegnati ed i relativi numeri seriali impressi al loro interno.
Acronimo **Fp**

Fornitori di bande laser: *Aziende produttrici della banda ottica a lettura laser.*
Provvedono alla fornitura delle bande ottiche a lettura laser, durante il processo di produzione imprimono, tramite scrittura laser, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco.
Ogni consegna di lotti di bande ottiche, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di bande ottiche consegnate ed i numeri seriali impressi al loro interno.
Acronimo **Fb**

Istituto Poligrafico e Zecca dello Stato: *Ente a cui è riservata la produzione del documento e il supporto alla sua diffusione*
Provvede alla manifattura dei supporti fisici, all'inserimento (embedding) della banda ottica e del microprocessore nel supporto fisico, nonché alla inizializzazione elettrica di quest'ultimo.
Memorizza nel chip, ai fini della garanzia di autenticità, nella banda ottica tramite laser il numero d'identificazione univoco su

scala nazionale, fornitogli dal Sistema di Sicurezza del C.N.S.D., ed inscindibilmente legato ad essa.
Imprime lo stesso numero con tecnologia “Laser engraving” sul supporto fisico e stampa gli elementi grafici costanti (logo, sfondo, etc.).
Contabilizza i numeri seriali che identificano il lotto e la data di produzione del chip e della banda ottica.
Garantisce la logistica di distribuzione dei supporti.
Relativamente agli apparati forniti dall’Istituto, garantisce:

- la logistica di distribuzione assicurando, in fase di staging, il caricamento sugli apparati dei software di sicurezza del circuito di emissione forniti dal Ministero dell’Interno;
- che le postazioni di emissione CIE (sia di front-office che di back-office) siano correttamente configurate con i software forniti dal Ministero dell’Interno prima della loro consegna sul territorio;
- la consegna, l’installazione e l’attivazione degli apparati presso i Comuni dotati di CAPA secondo i relativi livelli di servizio;
- per quanto di competenza i servizi di manutenzione relativi agli apparati in tutte le loro componenti e i relativi livelli di servizio;
- la fornitura dei servizi di supporto tecnico e informativo ai Comuni relativamente alle attività e prodotti di competenza dell’Istituto.

Garantisce i CAPS e ne gestisce direttamente il funzionamento per la personalizzazione e stampa delle CIE dei Comuni non dotati di CAPA in base alle specifiche tecniche e livelli di servizio definiti ai sensi del presente decreto.
Trasmette le informazioni risultanti dalle procedure di inizializzazione al Sistema di Sicurezza del C.N.S.D.
Gestisce il Centro Servizi di Informazione e logistica (CSI), che coordina i processi di produzione dei supporti CIE, gestisce i flussi di approvvigionamento dei supporti e ospita un portale informativo per la gestione di informazioni logistiche.

Può provvedere allo sviluppo, per quanto di competenza, di servizi

fruibili tramite CIE.
Acronimo **IPZS**

Ministero dell'Interno

Ente che fornisce le infrastrutture tecnologiche centrali e garantisce la sicurezza dell'intero circuito di emissione, nonche' il servizio di validazione dei certificati digitali di autenticazione della CIE e il servizio ai cittadini per il blocco delle carte smarrite o rubate

Il Ministero dell'Interno, avvalendosi del C.N.S.D., cura la realizzazione, la gestione e manutenzione del Sistema di Sicurezza del C.N.S.D., della CA del C.N.S.D. e del S.S.C.E – Sistema di Servizi del Circuito di Emissione.

Al fine di garantire la sicurezza dell'intero circuito di emissione ha la responsabilità di verificare e certificare qualunque operazione che comporti l'inserimento, la modifica o la cancellazione delle informazioni (in particolare i dati identificativi) memorizzate sul microprocessore o sulla banda ottica, eccezion fatta per i dati relativi alla predisposizione ed erogazione dei servizi.

Ai fini della garanzia di autenticità, genera per ogni carta un numero di identificazione univoco, su scala nazionale, che trasmette all'Istituto.

Gestisce la sicurezza del circuito di emissione e fornisce i software di sicurezza e di emissione - che garantiscono anche l'anonimato dei flussi di emissione - che l'Istituto dovrà installare sugli apparati dallo stesso forniti durante la fase di staging preliminare alla consegna degli apparati stessi.

Identifica le postazioni di emissione CIE e il relativo software verificandone e attestandone la conformità prima della loro distribuzione sul territorio.

Rende disponibili gratuitamente i software di sicurezza e di emissione a tutti i Comuni o Uffici Consolari che si dotino di postazioni aggiuntive rispetto a quelle ricevute dall'Istituto, purché conformi alle specifiche pubblicate sul sito.

Gestisce i processi di verifica della congruità tecnica e della conformità degli standard e delle tecnologie utilizzate dall'Istituto nel processo di produzione, di approvvigionamento degli apparati di emissione e di gestione della logistica di dispiegamento degli apparati stessi.

Tramite collegamenti telematici consente alle singole Questure e ai Comuni di accedere ai documenti, conservati in forma cifrata presso il Sistema di Sicurezza.
Garantisce il monitoraggio e la relativa contabilizzazione delle carte utilizzate durante i processi di emissione e dei relativi flussi finanziari dei pagamenti, comunicando periodicamente i dati al Ministero dell'economia e delle finanze.
Garantisce il monitoraggio e la vigilanza in merito all'utilizzo degli apparati di emissione.
Distribuisce e mantiene aggiornato il file system della CIE.
Rende disponibile, per garantire l'autenticazione forte per l'accesso ai servizi con CIE, un'infrastruttura OCSP di verifica della validità dei certificati digitali delle CIE.
Rende disponibili i servizi di verifica della validità della CIE rispetto alla sua qualità di documento di riconoscimento dell'identità personale, costantemente aggiornati dai servizi di sicurezza del C.N.S.D..
Definisce i requisiti dei Piani di sicurezza, relativi ai processi di emissione, dei diversi soggetti coinvolti nel processo di emissione.
Vigila sulla applicazione dei Piani di Sicurezza.
Coordina le diverse componenti coinvolte nel progetto e, nel caso rilevi anomalie, malfunzionamenti e/o disservizi predispone le azioni correttive anche avvalendosi del comitato di cui all'art. 8-ter.
Assicura azioni di comunicazione, assistenza e supporto per i Comuni ai fini del popolamento dell'INA, dell'allineamento dei codici fiscali e della risoluzione di anomalie dell'archivio INA.
Il Ministero dell'Interno, con decreto ministeriale del 23 aprile 2002 ha costituito il Centro nazionale dei servizi demografici (C.N.S.D.), per gestire in modo integrato e razionale i flussi delle informazioni anagrafiche necessari al mantenimento dell'allineamento dei dati dell'anagrafe comunale, requisito essenziale ad una corretta gestione dei circuiti di emissione ed uso del documento. I Comuni si collegano su rete Internet o SPC al C.N.S.D. attraverso la porta di accesso ai servizi del C.N.S.D.. Rende disponibile i servizi di CA e di sicurezza e controllo per il circuito di emissione CIE e il circuito di accesso ai servizi tramite CIE.

Centri di Allestimento e Personalizzazione Autonomi.

Forniscono i servizi di allestimento, personalizzazione e stampa delle CIE per i Comuni emettitori

I Centri di Allestimento e Personalizzazione Autonomi, realizzati anche in forma associata tra i Comuni, forniscono servizi di personalizzazione e stampa delle CIE per i Comuni autonomi e gli Uffici Consolari.

Acronimo: **CAPA**.

Centri di Allestimento e Personalizzazione Sussidiari

Forniscono i servizi di allestimento, personalizzazione e stampa delle CIE per i Comuni che non usufruiscono di CAPA o in modalità backup per i CAPA

I Centri di Allestimento e Personalizzazione Sussidiari offrono, secondo modalita' asincrone, servizi di personalizzazione e stampa delle CIE per i Comuni che non stampano in autonomia le CIE.

Le funzioni di acquisizione dei dati dei cittadini richiedenti e le funzioni di attivazione e di rilascio della CIE al cittadino resta di pertinenza di ciascun Comune emittente. Acronimo: **CAPS**.

Emettitore:

Ente responsabile della formazione e del rilascio.

E' il Comune al quale il cittadino si rivolge per richiedere la CIE o un Ufficio Consolare cui il cittadino italiano residente all'estero si rivolge per richiedere la CIE.

Acronimo **E**

3 Infrastrutture tecniche e di rete

3.0 Sito della carta d'identita' elettronica.

Il sito Internet del documento e' raggiungibile all'indirizzo www.interno.it Tale sito e' curato dal Ministero dell'Interno ed e' il riferimento ufficiale per le specifiche tecniche di dettaglio del documento.

3.1 Dotazioni del C.N.S.D. (fa riferimento all'art. 6 del D.M.)

Ai i fini dell'emissione e dell'uso del documento, Il C.N.S.D. si compone di:

- connessione alle reti di accesso;
- funzioni di «security service provider» per consentire l'accesso, con modalita' di sicurezza, dei Comuni e agli Uffici Consolari;
- rete di accesso alle Questure per consentire la visualizzazione e la stampa dei cartellini elettronici alle Questure competenti;
- connessione sicura con IPZS per l'interscambio d'informazioni nella fase d'inizializzazione;
- connessione sicura, con le modalità specificate nel successivo art. 3.2.3, con i CAPS e i CAPA per l'interscambio d'informazioni nelle fasi di formazione;
- sistema dei servizi del circuito di emissione, per le funzionalita' centrali connesse alle diverse fasi di formazione della CIE;
- Sistema di sicurezza del C.N.S.D., per le funzionalità di sicurezza connesse alle diverse fasi di formazione della CIE;
- Sistema di contabilizzazione del C.N.S.D., per la contabilizzazione delle carte utilizzate durante i processi di emissione e dei relativi flussi finanziari dei pagamenti. Comunica periodicamente i dati al Ministero dell'economia e delle finanze e al CSI;
- CA del C.N.S.D., per le funzionalità di certificazione e firma connesse alle diverse fasi di formazione della CIE;
- connessione alle reti Internet e al sistema pubblico di connettività - SPC;
- servizi di porta applicativa per l'accesso, su backbone del C.N.S.D., ai servizi del C.N.S.D.;
- Servizi di porta di dominio per le funzioni di cooperazione tra C.N.S.D. (erogatore del servizio) e altre amministrazioni (fruitori del servizio).
- Servizi di monitoraggio e allarme su tutte le postazioni di emissione CIE presso i

Comuni e i relativi CAPA.
- Servizi di monitoraggio e allarme per tutte le Comunicazioni telematiche tra C.N.S.D. e CAPS.

3.2 Dotazioni dei Comuni

3.2.1 Dotazioni hardware (fa riferimento all'art. 10, comma 1 del D.M.)

La configurazione degli apparati hardware e dei prodotti software necessari per la formazione della CIE e' riportata presso il sito della Carta d'identita' elettronica. Presso tale sito il Ministero dell'Interno rendera' disponibile l'elenco delle apparecchiature omologate come idonee per il rilascio della Carta d'identita' elettronica.

3.2.2 Dotazioni software applicativo (fa riferimento all'art. 6, comma 1 del D.M.)

1. I Comuni, per le attivita' inerenti la formazione ed il rilascio delle CIE, saranno dotati di specifico software di sicurezza e di emissione, sviluppato dal Ministero dell'Interno e distribuito dal C.N.S.D..
Tale software avra' la possibilita' di interoperare con i sistemi informativi dei Comuni. Il Ministero dell'Interno rende disponibile, secondo le modalita' descritte sul sito, sia il software specifico della porta applicativa per l'accesso su backbone C.N.S.D. ai servizi del C.N.S.D., sia il software di supporto all'uso del documento da parte dei cittadini e delle Amministrazioni (librerie dei metacomandi. CSP e PKCS11).
2. I CAPS, tenendo conto delle funzioni del CSI, per le attività inerenti la formazione delle CIE saranno dotati di specifico software applicativo di sicurezza, di cui all'art. 6, comma 1., per le comunicazioni sicure con il C.N.S.D., sviluppato dal Ministero dell'Interno e distribuito dal Sistema di Servizi del Circuito di Emissione.

3.2.2-bis Modalita' di accesso ai servizi fruibili tramite il documento

Presso il sito della carta d'identita' elettronica sono descritte le modalita' per accedere ai servizi che richiedono l'utilizzo del documento.

3.2.2-ter Dotazioni per i cittadini.

Presso il sito della Carta d'identita' elettronica sono descritte le configurazioni necessarie per

accedere ai servizi di e-government mediante la Carta d'identita' elettronica da postazioni private.
Presso tale sito e' inoltre possible reperire e scaricare il software di integrazione necessario per utilizzare le funzioni della Carta d'identita' elettronica con i piu' diffusi ambienti software per personal computer.

3.2.3 Modalità di connessione al C.N.S.D.

L'interconnessione al C.N.S.D. avverrà secondo le seguenti modalità di trasporto:
- Tramite sistema pubblico di connettività (SPC)
- tramite altre reti a cui sono connesse le amministrazioni locali (ove non siano disponibili servizi SPC);
- tramite Internet.

In tutti i casi e' necessario l'utilizzo del software di sicurezza ai fini del processo di emissione della CIE e per avvalersi dei servizi applicativi del CNSD.
Il software per i Comuni consente di eseguire le funzioni necessarie per l'acquisizione dei dati riferiti alla persona del titolare, per la formazione del documento, e quelle per operare, con modalità di sicurezza, le connessioni al C.N.S.D.
Il software per i CAPS consente di eseguire le funzioni necessarie per operare, con modalità di sicurezza, le connessioni al C.N.S.D.
L'interconnessione al C.N.S.D. avverra' su backbone attraverso la porta applicativa di accesso ai servizi del C.N.S.D. secondo le seguenti modalita':
- tramite SPC;
- tramite altre reti a cui sono connesse le amministrazioni locali;
- tramite rete Internet.

In tutti i casi, e' necessario l'utilizzo della porta applicativa che, attraverso le quantità di sicurezza fornite dalla CA, si collega in modalità sicura al C.N.S.D.

4 Materiali e standard di riferimento

4.0 Uso del documento.
In considerazione della natura del certificato CIE che non contiene informazioni anagrafiche, e' necessario prevedere la definizione di meccanismi standard per garantire l'accesso ai servizi ai cittadini. In particolare, per garantire l'accesso ai servizi verranno definite modalita' operative che permettono l'estrazione dei dati anagrafici da inviare al web server che eroga i servizi, per implementare l'accesso basato su CIE, dai client verso i web server.

A tal fine verranno forniti da parte del Ministero dell'Interno, in logica open source, gli opportuni codici software.
In una fase transitoria, per le CIE prodotte in data antecedente all'entrata in vigore del presente decreto, per motivi di opportunita' o di incompatibilita' tecnologica del client del cittadino richiedente con le modalita' operative adottate, al termine della fase di challenge tra il client ed il web server nella quale viene scambiato esclusivamente il certificato della CIE, i web server possono richiedere, attraverso i servizi di convalida del backbone C.N.S.D., il codice fiscale corrispondente all'ID carta del cittadino direttamente al C.N.S.D.

4.1 Supporto fisico (fa riferimento all'art. 7, comma 1 del D.M.)

4.1.1 Dimensioni nominali e le componenti

Il supporto fisico deve essere conforme alle norme che regolamentano i Documenti di Identità International Standards Organization (ISO)/IEC 7816-1, 7816-2 .

Le dimensioni nominali dovranno essere di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810: 1995 per la carta di tipo ID-1. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.

Lo spessore della CIE, compresi i film di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 1995.

La CIE, sarà costituita da materiali plastici compatibili con gli strumenti tecnologici in essa contenuti, nonchè con i sistemi di personalizzazione utilizzati per la sua compilazione.

La CIE, per un uso normale nel periodo di validità, dovrà rispondere alle specifiche definite:

- nella norma ISO/IEC 7810: 1995 relativamente a: deformazioni, tossicità, resistenza ad agenti chimici, stabilità dimensionale ed inarcamento con temperatura e umidità, inarcamento con l'uso, infiammabilità e durata.
- nella norma ISO/IEC 11693 per la contaminazione, per la trasmissione della luce attraverso lo spessore della carta e per la resistenza agli agenti atmosferici ed ai test di compatibilità con l'ambiente.

Per quanto attiene alla presenza del microchip la CIE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite nella norma ISO/IEC 7816 - 1.

L'area a memoria ottica della CIE, per un normale uso durante il periodo di validità, deve rispondere alle specifiche definite dalle norme ISO/IEC 11693, 11694-1, 11694-2, 11694-3, 11694-4.

4.2 Carta a memoria ottica (fa riferimento all'art. 8, comma 1 del D.M.)

La carta ottica è realizzata in policarbonato, un materiale plastico di provenienza aeronautica, 1.000 volte più resistente del PVC, che garantisce un'ottima trasparenza per la scrittura su banda ottica, una elevata resistenza, una maggiore durata nel tempo ed un intervallo termico di utilizzo molto ampio (-40° +100°).
Il film è composto da diversi strati di materiale ed il supporto ottico registrabile è incapsulato tra due livelli di materiale protettivo trasparente che (sulla faccia esterna) è rinforzato da un ulteriore strato "antigraffio".

La capacita' di memoria della carta ottica utilizzata, nella dimensione adottata, è di circa 1,8 MByte.

Ogni carta ottica permette la creazione di settori variabili basati su tracce, consentendo così l'archiviazione di informazioni multiple ed indipendenti.

Le carte ottiche, rispondono allo standard ISO/IEC 11694.

4.3 Microprocessore (fa riferimento all'art. 8, comma 1 del D.M.)

E' composto da un circuito stampato, che esercita le funzioni di interfaccia verso l'esterno, e da un circuito integrato (chip), incastonati sulla scheda.

In particolare per la CIE sono ammissibili, per un periodo transitorio, tagli di memoria EEPROM da almeno 32KBytes e algoritmi RSA, per operazioni di crittografia asimmetrica, almeno a 1024 bit. A regime, tenendo conto delle tecnologie disponibili, dovranno essere utilizzati tagli di memoria EEPROM da almeno 64KBytes e con algoritmi RSA almeno a 2048 bit.

Per la CIE sono inoltre ammissibili, per la crittografia asimmetrica, algoritmi RSA da almeno 1024, 2048, o 3072 bit e algoritmi ellittici ECDSA con curve raccomandate da 224 a 283 bit.

Il Comitato di Indirizzo indica, sulla base di quanto definito dal Comitato Tecnico Scientifico Permanente di cui all'art. 8 bis, gli aggiornamenti da apportare a tali requisiti tecnologici dei microprocessori della CIE.
Il chip deve essere conforme alle specifiche definite nel protocollo di intesa Ministero dell'Interno, Ministero per le riforme e le innovazioni del 13 maggio 2003 e successive modificazioni, nonché alle specifiche definite dal Comitato Tecnico Ristretto CIE a completamento dei suoi lavori sul microchip della CIE, in data 21 aprile 2006.
Il Chip deve rispondere al reset con una sequenza ATR, che deve contenere una sottosequenza di caratteri che identifichi in modo inequivocabile la versione del microprocessore e che si tratta di carta d'identita' elettronica italiana. La sequenza ATR è definita ed aggiornata dal Comitato Tecnico-Scientifico Permanente e pubblicata sul sito.

Il chip della CIE deve essere almeno a tecnologia contact, secondo lo standard ISO 7816.

Sulla base dell'evoluzione delle tecnologie, potranno essere utilizzati dispositivi funzionanti anche senza contatti e operativi a distanze inferiori ai 10 cm, la cui usabilità sarà valutata sia sulla base dell'evoluzione degli standard e dei risultati dei processi di innovazione tecnologica, sia sulla loro adeguatezza ai livelli di sicurezza e protezione della privacy previsti per la carta d'identità elettronica. L'attivazione di questa modalità di funzionamento dei dispositivi potrà avvenire solo a fronte del diretto assenso del cittadino.

Il microprocessore a bordo della CIE deve quindi essere almeno conforme ai seguenti standard di riferimento:
ISO 7816-3
ISO 7816-4
ISO 7816-8
E successivi aggiornamenti.

Il microprocessore a bordo della CIE deve inoltre:

a) rispettare tutte le specifiche riportate nel presente documento;
b) rispettare le specifiche del sistema operativo (APDU) pubblicate sul sito;
c) aver superato i test di compatibilita' predisposti dal Ministero dell'Interno ed effettuati dalla Commissione di verifica e omologazione tecnica di cui all'art. 8 quater.

A tal fine ogni fornitore di chip dovra' realizzare e rendere disponibile al Ministero dell'Interno un ambiente di test per il chip che consenta di verificare tutte le funzionalita' richieste dal Ministero e dichiarate dal fornitore per il chip stesso, sia per le fasi di inizializzazione, sia per successive fasi di rilascio ed uso, nonche' per installazione ed uso di firma elettronica. Tale ambiente sara' utilizzato dal laboratorio di sicurezza del C.N.S.D., che opera sotto la direzione del responsabile del coordinamento scientifico e progettuale dei progetti C.N.S.D. e CIE, per le verifiche del caso.

Le procedure idonee alle verifiche di compatibilità di cui al punto c) sono pubblicate sul sito del Ministero. La verifica di compatibilità è a titolo gratuito e la procedura viene espletata entro 30 giorni solari dalla richiesta.
Il Ministero dell’Interno pubblica il file system della CIE.

4.4 Dati (fa riferimento all’art. 13, comma 1, lettera d del D.M.)

Di seguito è riportato il formato elettronico dei dati previsti nella CIE.

Descrizione campo	Tipo
Numero assegnato al documento in bianco..	carattere
Comune che emette il documento....	carattere
Data di emissione del documento...	carattere data
Data di scadenza del documento....	carattere data
Cognome....	carattere
Nome....	carattere
Data di nascita....	carattere data
Sesso....	carattere (M/F)
Statura (cm.)....	carattere

Codice fiscale....	carattere
Cittadinanza....	carattere
Comune/Stato estero di nascita....	carattere
Estremi atto di nascita....	carattere
Comune di residenza....	carattere
Indirizzo....	carattere
Firma del titolare....	BMP JPG (fattore 5)
Eventuale annotazione in caso di non validita' del documento per l'espatrio....	Logico
Fotografia 23 x 28 mm. - 200 dpi 16 Ml di colori (a 24 bit)....	BMP JPG (fattore 5)
Impronte digitali del dito indice di ogni mano 1 "x1" - 500 dpi - 256 liv. di grigio (ove, in una mano, l'impronta del dito indice non fosse disponibile si utilizzera' per la stessa, procedendo in successione: la prima impronta disponibile fra le dita: medio, anulare e mignolo)....	BMP WSQ
Template impronte digitali....	numerico

La dimensione, i formati di dettaglio ed i relativi livelli di protezione, dei vari campi indicati nella tabella, saranno definiti a seguito della elaborazione delle specifiche tecniche di dettaglio e pubblicati sul sito.
In particolare nella memoria del microprocessore della CIE sono ammissibili aree di memoria destinate alla memorizzazione opzionale delle impronte digitali, in associazione alle apposite sezioni previste per la memorizzazione opzionale dei template numerici delle impronte digitali.
Le impronte digitali e i relativi template restano utilizzabili solo per la finalità di verifica dell'identità del titolare del documento e non sono in ogni caso registrati in banche di dati.

La struttura del certificato di autenticazione della CIE, per tenere conto delle esigenze di interoperabilità con il certificato di autenticazione della carta CNS, e in aderenza agli standard tecnici comunemente adottati, è modificata come di seguito descritto:

- il codice fiscale del titolare è inserito nel campo Common Name del Subject (DN), pubblico, per compatibilità con il certificato della CNS;
- il codice identificativo del microchip della CIE (che riporta, in modalità alfanumerica, produttore, tipo e versione del microchip), separato dal codice fiscale tramite il carattere "."(dot, ASCII 0x2E), è inserito nel campo Common Name del Subject (DN);
- l'identificativo univoco del dispositivo (ID_Carta), cifrato con chiave di cifra emessa e gestita dal Ministero dell'Interno, riportato in base 64, è inserito nel campo DNQ(dnQualifier) del Subject (DN), con sintassi di tipo PrintableString;
- il campo emailAddress dell'attributo X509v3 "Issuer Alternative Name" è valorizzato con support@backbone.cnsd.interno.it.
- il valore dell'hash, calcolato sul file elementare contenente i dati riferiti alla persona del titolare, riportato in base 64, è inserito nel campo serialNumber del Subject (DN), con sintassi di tipo PrintableString(1..64);

Tale soluzione è necessaria anche per aderire alle prescrizioni degli organismi internazionali di definizione degli standard per la sicurezza che prevedono, per gli enti governativi, la sostituzione, a partire dal 2010, della cifratura asimmetrica RSA 1024 bit in RSA 2048 bit e degli algoritmi di hash della famiglia denominata SHA-1 con quelli della famiglia denominata SHA-2, di cui ne consigliano, ove possibile, l'utilizzo fin da subito.

A tal fine, nei certificati CIE:

- l'hash del file elementare contenente i dati riferiti alla persona del titolare deve essere calcolato utilizzando almeno l'algoritmo sha224 e, riportato in base 64, memorizzato nel campo serialNumber del Subject ID.
- il "Signature Algorithm" della CA del CNSD, attualmente valorizzato a "sha1WithRSAEncryption" è sostituito con il "Signature Algorithm" "sha224WithRsaEncription" o superiore.

È previsto un periodo transitorio per la completa attivazione sul territorio della modifica del certificato di autenticazione della CIE.

Ai fini della verifica dei certificati digitali delle CIE, il C.N.S.D. rende disponibili servizi O.C.S.P. (RFC 2560 e successivi aggiornamenti), accessibili anche per il tramite del Sistema Pubblico di Connettività (SPC).

5 Misure di sicurezza (fa riferimento all'art. 4 del D.M.)

Questo paragrafo descrive le misure adottate, durante tutte le fasi della produzione e dell'utilizzo della CIE, per ottenere i corretti livelli di sicurezza e di interoperabilità della carta.

5.1 Sicurezza del supporto fisico

Nel seguito sono elencati gli elementi utilizzabili per la sicurezza del supporto e per accertarne l'autenticità, anche attraverso il semplice esame visivo.

5.1.1 Elementi di sicurezza grafici e di stampa

E' previsto l'uso dei seguenti elementi di sicurezza, tipici delle carte valori:

- motivi grafici ad elementi variabili;
- elementi grafici diffrattivi;
- microprint;
- processo di masterizzazione photomask con stampa ad alta risoluzione di immagini direttamente su film ottico;
- embedded hologram (incisione grafica su banda laser);

5.1.2 Inchiostri

Per la stampa è previsto l'impiego di inchiostri dotati di speciali caratteristiche, come quelli fluorescenti (visibili all'ultravioletto) e otticamente variabili (OVI - Optical Variable Ink).

5.1.3 Numerazione di serie

La numerazione del documento in bianco, realizzata con sistema ad incisione laser sul fronte del documento, è ripetuta visibilmente sulla banda ottica con il sistema dell' "embedded Hologram", memorizzata al suo interno ed inserita come dato all'interno del microprocessore.

5.1.4 Applicazione di elementi Optical Variable Device (OVD)

Sul retro del documento, nella fase di produzione, è applicato a caldo un ologramma di sicurezza.

5.2 Sicurezza della fase di personalizzazione

Al fine di consentire la stampa della CIE presso i Comuni o i CAPS ad un costo contenuto, la tecnica da utilizzare è quella della termografia a colori (eventualmente apponendo uno strato neutro intermedio).

Anche la compilazione grafica sarà uniforme per tutto il territorio nazionale tramite l'utilizzo di caratteri, provenienti da un unico "font" appositamente realizzato per la CIE che verrà distribuito unitamente al software di sicurezza, dal C.N.S.D..

Inoltre, l'apposizione di embedded hologram (incisione grafica su banda laser) consente di replicare, su banda ottica, i dati identificativi del titolare del documento, al fine di rendere più sicura l'identificazione a vista.

Infine, come accennato, al termine della stampa termografica, il processo prevede l'applicazione sul fronte di un "overlay" di protezione di spessore compreso tra 12,5 e 25,0 micron al fine di offrire ulteriori sicurezze e garantire la durata oltre i cinque anni.

5.3 Affidabilità dei dati

5.3.1 Laser su banda ottica

I dati vengono memorizzati permanentemente sulla banda laser (sistema WORM) in formato digitale e letti/scritti con appositi apparati, detti lettori/scrittori.

5.3.2 Microcircuito

Le informazioni memorizzate sul microprocessore sono:

- le informazioni specifiche dell'hw e del sw;
- le informazioni anagrafiche del titolare;
- dati individuali aggiuntivi;
- dati relativi ai singoli servizi;
- template opzionale dell'impronta.

L'accesso a queste ultime tre tipologie di dati e' possibile solo dopo il consenso del titolare

espresso ordinariamente tramite digitazione di PIN.
I dati individuali aggiuntivi sono informazioni relative al titolare che sono registrate sulla carta, ad integrazione delle informazioni anagrafiche, e che possono essere utilizzate ai fini dell'erogazione dei servizi.
Queste informazioni estendono l'identita' del titolare, non sono specifiche di un servizio e non sono modificabili a seguito dell'erogazione dei servizi.
Vengono registrate o modificate sulla carta esclusivamente dal Comune su esplicita richiesta del titolare e, in pratica, abilitano la carta all'accesso a quei servizi delle amministrazioni locali e centrali la cui erogazione necessita di tali dati.
I dati relativi ai singoli servizi qualificati sono informazioni registrate sulla carta, eventualmente modificabili durante l'erogazione del servizio, e relative ad attributi del titolare della carta che sono funzionali esclusivamente all'amministrazione erogante il servizio.

5.4 Sicurezza del circuito (fa riferimento all'art. 6, comma 1 del D.M.)

La migliore garanzia contro tentativi di falsificazioni e utilizzo di carte rubate si trova nella centralizzazione virtuale prevista dall'architettura del circuito d'emissione della CIE.

In tale logica, il Sistema di Sicurezza traccia tutte le operazioni al fine di garantire il rispetto della normativa vigente sulla riservatezza delle informazioni e dei dati riferiti alla persona, per impedire l'emissione di documenti falsi e per individuare facilmente l'utilizzo fraudolento di documenti rubati e la contraffazione di documenti autentici.

Nel capitolo 7 verranno descritte dettagliatamente tutte le fasi del processo di emissione.

5.4.1 Sicurezza degli accessi ai dati (fa riferimento all'art. 6 del D.M.)

In base al Regolamento di esecuzione del Testo Unico delle Leggi di P.S. (Regio decreto 18 giugno 1931, n. 773 e successive modificazioni), oltre al titolare possono accedere alle informazioni contenute nei documenti esclusivamente i Comuni, che emettono le carte d'identità, e le Questure competenti territorialmente. Infatti, sia gli uni che gli altri sono tenuti a conservare copia dei documenti emessi.

Passando da un documento cartaceo ad uno di formato elettronico, anche la copia conservata da Comune e Questura (cartellino cartaceo) diviene di tipo digitale (cartellino elettronico).

Pertanto, a fini di sicurezza e nel rispetto delle norme di legge, la "base dati" Comune consente

l'accesso e la visualizzazione dei cartellini elettronici al solo Comune di residenza ed alla Questura territorialmente competente.

A tal fine il Sistema di Sicurezza del C.N.S.D. garantisce la tracciabilità di tutte le attività, relative ai dati identificativi, per ogni singolo documento, consentendo di risalire, in qualsiasi momento, alle informazioni di "chi ha fatto cosa e quando", nel rispetto delle attuale normativa, durante tutte le fasi di formazione, compilazione, rilascio, rinnovo ed aggiornamento dei documenti.

Il Sistema di Sicurezza, grazie ad un meccanismo di cifratura basata su algoritmo a chiave asimmetrica, non è in grado esso stesso di accedere ad alcuna informazione di carattere personale che può essere visualizzata, tramite la propria chiave privata, esclusivamente dalla Questura o dal Comune competente.
Da un punto di vista tecnico, i dati sono prima cifrati per mezzo di un algoritmo simmetrico di provata robustezza (ad es. 3DES) con una chiave di lunghezza non inferiore a 128 bit (generata in modalità casuale); quest'ultima, prima di essere distrutta, viene a sua volta cifrata sia con la chiave pubblica della Questura che con quella del Comune e memorizzata assieme all'informazione.

5.4.2 Sicurezza della carta

I rischi di utilizzo fraudolento e falsificazione delle carte d'identita', anche a causa di furti di carte «in bianco», con l'adozione del modello elettronico, sono notevolmente ridotti, principalmente in virtu' della natura del supporto e delle garanzie di inalterabilita' delle informazioni riportate, tanto sul chip che sulla banda ottica.
La banda ottica rappresenta un elemento centrale della sicurezza per i motivi di seguito riportati. La caratteristica di base della scrittura WORM (Write Once Read Many) non permette alterazioni, realizzate mediante la cancellazione di dati e la loro sostituzione con altri. Infatti, le informazioni memorizzate non sono cancellabili e riscrivibili. Eventuali aggiornamenti consistono esclusivamente in aggiunte, proprio come avviene per un normale CD-ROM.

In ogni caso esistono gli standard di sicurezza e le protezioni inserite nell'hardware, in dotazione esclusivamente a E. CAPS ed IPZS, e di ogni operazione effettuata dal funzionario autorizzato con modalita' gestite elettronicamente, si tiene traccia presso il C.N.S.D.

Il controllo a vista della carta, inoltre, e' garantito dalla presenza dell'Embedded Hologram che permette di effettuare un'azione di costante validazione dei dati stampati in chiaro e di evidenziarne immediatamente il tentativo di manomissione.

Relativamente al microchip, questi non permette - grazie alla sicurezza del suo stesso sistema operativo - di modificare o scrivere informazioni se non in presenza di determinate autorizzazioni. Inoltre tutte le informazioni sensibili, tanto sul chip che sulla banda ottica, sono garantite contro l'alterazione, perche' «firmate» digitalmente.

5.4.3 Furto della carta "attivata" o documento in bianco

La carta è in tale stato quando viene inviata da IPZS ai Comuni o ai CAPS, prima di essere formata e rilasciata.
In questo caso, dal momento che la personalizzazione richiede, per poter aver luogo, l'autenticazione del funzionario nei confronti del sistema e la firma dei dati da parte di appositi apparati contenenti la chiave privata dell'ente, tale eventualità rientra nella tipologia del "rilascio fraudolento" realizzabile solo attraverso l'infedeltà del funzionario stesso le cui attività però, con la citata tracciatura, restano registrate nel Data Base delle approvazioni presso il C.N.S.D.

5.4.4 Controlli a vista

L'intero circuito di sicurezza attraverso l'adozione dell'architettura a centralizzazione virtuale consente di innalzare il livello di qualità dei controlli, c.d. a vista, effettuati dalle Forze di Polizia per verificare l'identità delle persone sottoposte ai controlli stessi.

Disporre di un documento particolarmente attendibile consente di eseguire tutte le normali procedure in tempi molto ridotti con indubbio vantaggio per le persone coinvolte.

Le sicurezze adottate durante la fase di inizializzazione del documento, la presenza sulla banda ottica, sotto forma di ologramma, delle stesse informazioni grafiche, lo rendono molto più affidabile del modello cartaceo.
Laddove si volessero approfondire le verifiche, due sono le possibili soluzioni:

• Controllo dei dati autenticati e memorizzati nella banda ottica. Tramite apposito lettore opportunamente inizializzato, in grado di rilevare con certezza l'autenticità del documento
• Controllo delle informazioni presso la CA del C.N.S.D.. Le Questure di competenza possono, collegandosi al C.N.S.D., verificare immediatamente, grazie al possesso di opportune chiavi crittografiche, se le informazioni in esso contenute corrispondono con quelle riportate nel documento.

5.4.5 Lista dei documenti interdetti (fa riferimento all'art. 6, comma 2 del D.M.)

In attuazione dell'art. 6, comma 1, del D.P.C.M. del 22 ottobre 1999, n. 437, presso la CA del C.N.S.D. è presente un elenco dei documenti interdetti (black-list). Tale elenco è indispensabile per impedire l'operatività della CIE in caso di smarrimento o furto della stessa.
Le procedure da seguire per l'interdizione della carta vengono dettagliatamente descritte nei successivi paragrafi.

5.4.6 Software di sicurezza distribuito ai Comuni (fa riferimento all'art. 6, comma 1 del D.M.)

Per procedere alla formazione e all'emissione dei documenti, i Comuni e i CAPS devono collegarsi al C.N.S.D.. In assenza di tale collegamento qualsiasi documento prodotto verrebbe facilmente individuato come falso.
I requisiti per collegarsi al circuito di emissione sono un collegamento telematico, secondo i criteri stabiliti al paragrafo 3.2 del presente documento, e l'adozione di uno speciale software di sicurezza rilasciato dal Sistema di Sicurezza stesso.
Il Ministero dell'Interno cura l'analisi, lo sviluppo, la distribuzione e la manutenzione di tale software, per motivi di riservatezza, di interoperabilità e di economicità.
L'Istituto cura, in fase di staging, per le postazioni che fornisce direttamentel'installazione dei software di sicurezza e di emissione, forniti dal Ministero dell'Interno, sulle postazioni di acquisizione dati e sulle postazioni di allestimento e stampa destinate ai Comuni, Uffici Consolari e CAPA.

Il Ministero dell'Interno rende disponibili gratuitamente i software di sicurezza e di emissione a tutti i Comuni o Uffici Consolari che si dotino di postazioni aggiuntive rispetto a quelle ricevute dall'Istituto, purchè conformi alle specifiche pubblicate sul sito.
Le chiavi private del Comune o dei CAPS, la prima volta dovranno essere ritirate presso il Ministero dell'Interno o le Prefetture.
I software di sicurezza e i loro aggiornamenti potranno essere inviati, tramite modalità telematica, mediante meccanismi di "software distribution".

6 Servizi erogabili in rete (fa riferimento all'art. 5 del D.M.)

Le tipologie dei servizi erogabili possono, in sostanza, ricondursi a due: servizi standard, che non necessitano di essere installati sul documento e servizi qualificati che richiedono

l'installazione.
Nel caso dei servizi standard si accede al servizio con il semplice riconoscimento tramite digitazione del PIN o inserimento di altre quantità di sicurezza e l'utilizzo del certificato della carta per la strong authentication. I servizi standard vengono erogati in piena autonomia dalle amministrazioni interessate.
Richiedono invece l'installazione sulla carta, quei servizi (detti qualificati) che necessitano di informazioni aggiuntive da memorizzare sul microprocessore. L'installazione dei servizi qualificati e' effettuata presso i Comuni o strutture tecnologiche formalmente delegate dai Comuni, con l'eccezione del servizio di firma digitale disciplinato dal decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale. Tale servizio deve essere effettuato utilizzando un certificatore accreditato ai sensi del medesimo decreto.
Il Ministero dell'Interno, in conformità alla normativa vigente in materia e alle regole tecniche di cui all'art. 34 del decreto legislativo 7 marzo 2005, n. 82, genera direttamente certificati qualificati per la firma digitale dei pubblici ufficiali.
Tali certificati, installati all'interno della CIE possono essere utilizzati esclusivamente per le finalità di cui all'art. 34, comma 1, lett. A) del citato decreto.
Nelle CIE prodotte dalla data di pubblicazione di questo decreto, puo' comunque essere inserito almeno un altro certificato qualificato per la firma digitale, rilasciato al titolare per l'utilizzo in una diversa qualità o status personale, in conformità agli articoli 24 e seguenti del decreto legislativo 7 marzo 2005, n. 82 citato e alle regole tecniche vigenti in materia.
Ai Comuni, o a strutture tecnologiche formalmente delegate dagli stessi, spetta l'attivita' di registrazione per il riconoscimento certo del titolare ai fini di garantire la correttezza delle generalita' del soggetto per il quale, direttamente, ovvero ai sensi dell'art. 2, comma 1, del presente decreto, richiederanno al certificatore accreditato, con le modalita' stabilite dal Ministero dell'Interno di concerto con il Ministro per le riforme e le innovazioni nella PA, il rilascio di un certificato qualificato.
In caso di perdita del possesso o di compromissione della funzionalità della CIE, il titolare si attiene alle modalità operative ricevute dal Comune in fase di rilascio della CIE. Tale modalità operative conterranno anche, in presenza di un certificato qualificato rilasciato con la CIE, le indicazioni necessarie e le informazioni utili a richiedere la revoca del certificato di firma digitale al certificatore che lo ha emesso.

Il Ministero dell'Interno, stipulando apposite convenzioni con i certificatori accreditati, fornisce ai medesimi le modalità tecnologiche ed operative di inserimento nella CIE degli elementi inerenti il servizio qualificato di firma digitale, nonché le quantità di sicurezza necessarie per l'inserimento del certificato medesimo.
L'inserimento nella CIE dei certificati di firma digitale e delle relative quantità di sicurezza effettuata ai sensi del presente paragrafo non deve essere tale da introdurre, per ognuno dei differenti certificatori accreditati con i quali il Ministero dell'Interno stipulerà di volta in volta apposite convenzioni, diversità nei software o nelle modalità di utilizzo della CIE come strumento di firma digitale da parte dei cittadini né, tantomeno, da alterare i profili di protezione utilizzati per la certificazione di sicurezza dei supporti informatici della CIE, ai sensi dell'art. 52, comma 3, del decreto del Presidente del Consiglio dei Ministri, 13 gennaio 2004 e successive modifiche.

Nei certificati qualificati rilasciati ai titolari per l'utilizzo della firma digitale al di fuori delle finalità istituzionali, ai sensi dell'art. 28, comma 3, del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante "Codice dell'Amministrazione Digitale" possono essere contenuti, ove richiesto dal titolare o dal terzo interessato, se pertinenti allo scopo per il quale il certificato è richiesto informazioni relative a:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) del citato art. 28 comma 3;

c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

6.1 Le liste delle carte sospese e interdette (black-list)

Il C.N.S.D. rende disponibili lo stato di sospensione e di interdizione delle CIE e lo stato di revoca dei certificati digitali tramite OCSP (RFC 2560 e successivi aggiornamenti).

6.1-bis Le liste dei servizi qualificati

Le liste dei servizi qualificati e gli standard di caricamento e di interoperabilità sono approvati dal comitato di indirizzo e monitoraggio di cui all'art. 8ter del presente D.M. e pubblicati sul sito.

6.2 Modalità di riconoscimento in rete

Le modalità di erogazione del servizio di riconoscimento in rete sono definite dal Comitato di indirizzo e monitoraggio di cui all'art. 8ter del D.M. e sono dettagliate sul sito. Come specificato nel precedente punto 4.4, il campo common name del certificato della CIE contiene il codice fiscale del titolare, per garantire la compatibilità con le previsioni del punto 6.1.1 del Decreto 9 dicembre 2004 "Le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi."
Nell'attuazione dei servizi erogabili in rete non si procede in alcun caso al tracciamento e/o alla registrazione centralizzata presso il Ministero dell'Interno di dati relativi all'utilizzo della carta per l'accesso ai servizi delle PP.AA. né dei servizi per cui è stata richiesta l'autenticazione.

6.2.1 Crypto Middleware ed API PKCS11.

Il Cripto Middleware e' costituito dalle applicazioni (piattaforme) che il Ministero dell'Interno mette a disposizione dei Client, che operano su reti aperte, per gestire i servizi di cifratura/decifratura, verifica dello stato dei certificati e convalida anagrafica.
Orientativamente, tali piattaforme svolgono le seguenti funzioni:

- Richiesta di certificazione di chiavi pubbliche
- Richiesta di revoca certificati
- Accesso ai servizi di O.C.S.P. per la verifica dello stato del certificato digitale delle CIE;
- Accesso ai servizi di convalida anagrafica dei dati anagrafici presenti sulla CIE;
- Parsing dei Certificati Digitali
- Costruzione di strutture PKCS7
- Interfaccia ad alto livello verso le funzioni di cifratura.

Queste piattaforme, a loro volta, poggiano su strati software, o API, che le isolano dai dispositivi di cifratura, tipicamente le Smart Card.

Le API piu' comunemente usate sono le PKCS11, le cui caratteristiche salienti sono:

- Consentire ai Crypto Middleware di prescindere dai dispositivi che memorizzano chiavi e sviluppano crittografia
- Fornire ai Crypto Middleware una interfaccia standard
- Rendere portabili le applicazioni negli ambienti in cui la crittografia e' trattata con queste API.

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

6.2.2 Processo di Strong Authentication.

Questo processo consente l'identificazione da remoto della carta, la sua verifica e la convalida dei dati anagrafici ad essa associati, per la fruizione dei servizi erogati da una applicazione residente presso una Pubblica Amministrazione Centrale.

Orientativamente, i passi previsti dalla procedura sono:

1. L'applicazione client stabilisce la comunicazione con l'applicazione server.
2. L'applicazione server richiede all'applicazione client il file «C Carta» contenente il certificato.
3. L'applicazione client interroga la carta e legge tale file mediante i comandi APDU SELECT FILE (C Carta), READ BINARY.
4. L'applicazione client invia il file «C Carta» al server.
5. L'applicazione server verifica la validita' del certificato ed estrae da esso ID Carta e Kpub.
6. L'applicazione server accede ai servizi di convalida resi disponibili dal C.N.S.D. attraverso i punti di accesso delle richieste di validazione CIE, per verificare lo stato della CIE.
7. L'applicazione server, quando abilitata dal Ministero dell'Interno per le CIE prodotte in data antecedente all'entrata in vigore del presente decreto, accede ai servizi di convalida anagrafica resi disponibili dal C.N.S.D. per associare l'ID carta ai dati anagrafici del cittadino.
8. L'applicazione server genera una stringa di challenge e la invia al client rimanendo in attesa della risposta.
9. L'applicazione client seleziona Kpri mediante il comando MSE (Manage Security Environment). In tal modo Kpri e' attivata e verra' usata in tutte le successive operazioni di cifratura effettuate dalla carta. Mediante il comando PSO (Perform Security Operation) la carta esegue la cifratura del challenge usando Kpri precedentemente attivata, e restituisce all'applicazione client la stringa ottenuta. La chiave privata che e' stata generata dalla carta in fase di inizializzazione, risulta invisibile dall'esterno e comunque impossibile estrarla dalla carta.
10. Il client invia al server in attesa il challenge firmato ricevuto dalla carta.
11. L'applicazione server verifica la stringa ricevuta e la confronta con il challenge precedentemente generato. Se tale confronto ha esito positivo la carta e' autenticata. A questo proposito e' necessario che l'algoritmo di verifica, residente sul server, sia compatibile con quello usato dalla carta per cifrare il challenge.

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

6.2.3 Comandi di gestione utilizzati dalla Strong Authentication.

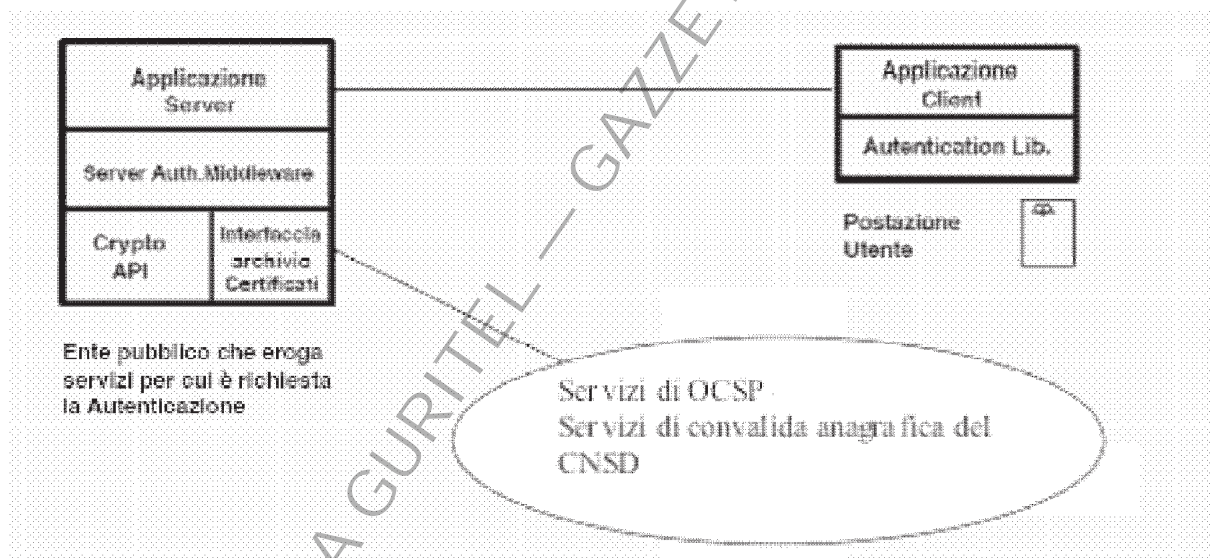
La norma ISO 7816 parte 4 e parte 8 definisce, oltre alla struttura del File System, anche i comandi per interagire a livello applicativo.

Tali comandi sono chiamati APDU (Application Protocol Data Unit). L'insieme delle APDU della CIE e' pubblicato sul sito del C.N.S.D., insieme alle librerie di gestione di tali APDU.

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

6.2.4 Strong Authentication lato Server.

Quanto affermato nei precedenti paragrafi e' un solido punto di partenza per risolvere il problema della autenticazione forte in rete per quanto concerne il Client e la CIE. E' ora necessario definire la componente server del processo di autenticazione.

La seguente figura illustra i componenti che intervengono nel processo di autenticazione.

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

7 Processo di Emissione

Nel presente capitolo sono descritte in le fasi operative di massima previste dal circuito d'emissione. Tutti gli aggiornamenti a tale schema di flussi saranno pubblicati sul sito.
Per una migliore comprensione del processo d'emissione si riporta un glossario di riferimento.

Fb	**Fornitori Bande Ottiche**
Fp	**Fornitori microprocessori**
IPZS	**Istituto Poligrafico Zecca dello Stato**
CA	**CA del C.N.S.D.**
Sistema di sicurezza	**Sistema di sicurezza del C.N.S.D.**
E	**Ente emettitore della CIE, Comune O CAPS.**
ID_Carta	**Numero identificativo della carta assegnato in modo indissolubile al documento d'identità e generato dal sistema di sicurezza**
C_Carta	**Certificato anticontraffazione della carta** **Unisce in maniera inscindibile i due supporti informatici.**
Dati_processore	**File elementare che riporta dati univoci del processore**
Dati_banda_ottica	**File elementare che riporta dati univoci della banda ottica**
Rd	**Record dati. area della banda ottica**
PIN P1	**Abilita l'accesso in scrittura ai files elementari (Securizza ulteriormente la fase di compilazione)**
PIN utente	**Abilita l'uso della chiave privata Kpri per le operazioni di autenticazione in rete.**
PUK Utente	**Abilita il titolare allo sblocco della carta e reimpostazione del PIN utente.**
PIN SO / Altre soluzioni equivalenti	**Abilita all'installazione della firma digitale sulla carta.**

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

7.1 Produzione di banda laser e microprocessore

I Fornitori di microprocessori (Fp) ed i Fornitori di bande ottiche (Fb) provvedono alla fabbricazione dei supporti informatici.
I Fornitori di microprocessori provvedono anche alla mascheratura in ROM del Sistema Operativo.

Entrambi i fornitori applicano, in fase di produzione, un numero seriale progressivo univoco, sui supporti informatici da loro forniti e predispongono una distinta, cartacea ed elettronica, che riporta le seguenti indicazioni: ID fornitore, numero seriale, numero del lotto di produzione, data di produzione.

I fornitori, successivamente, inviano i loro prodotti, accompagnati dalle distinte, direttamente all'Istituto Poligrafico dello Stato (IPZS).

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

7.2 Produzione ed inizializzazione della carta d'identita elettronica e del documento elettronico

Per meglio comprendere le diverse fasi del circuito di emissione, è bene fare dei brevi cenni sull'organizzazione e sulla normalizzazione delle informazioni sui supporti informatici della CIE.

7.2.1 Struttura delle informazioni sulla banda ottica

Sulla banda ottica vi sono due aree di memorizzazione differenti ma sincrone:

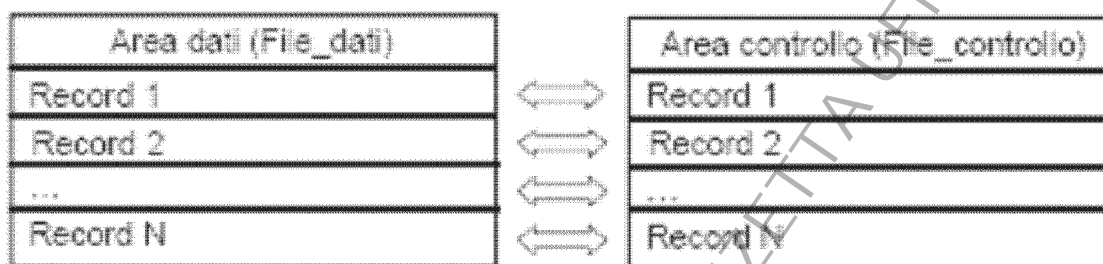
- Una area dati che contiene, codificati in record di formato opportuno (R_d), i necessari dati della carta, del titolare e i servizi installati.
- Una area di controllo che contiene, codificate in formato opportuno (R_c), le informazioni di controllo e verifica dei corrispondenti R_d.

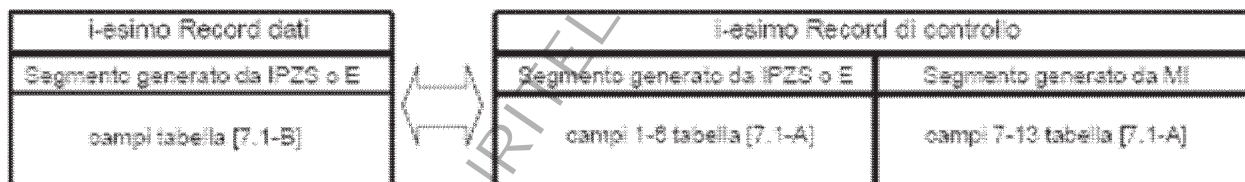
L'area controllo è assimilabile ad un registro incrementale delle operazioni avvenute sulla carta, e consente di stabilire con certezza *chi*, *dove* e *quando* ha effettuato ed autorizzato ogni operazione. La certezza viene stabilita dall'uso incrociato dei "sigilli" apposti da:

- Istituto Poligrafico dello Stato;
- Emettitori o CAPS;
- CA o Sistema di Sicurezza del C.N.S.D..

A ciascun record R_d dell'area dati corrisponde un record R_c dell'area di controllo. I record dati possono avere formati multipli secondo necessità.

I record R_d dell'area dati sono formati da **IPZS** e da **E**. I record R_c dell'area di controllo sono composti da due parti: una formata da **IPZS** e da **E**, l'altra formata dalla CA del C.N.S.D..

La successiva figura mostra l'organizzazione in record corrispondenti dell'area dati (File_dati) e dell'area di controllo (File_controllo):

La successiva figura mostra, invece, per ciascun record corrispondente dell'area dati e di quella di controllo, la suddivisione in campi:

i-esimo Record dati		i-esimo Record di controllo	
Segmento generato da IPZS o E	⟺	Segmento generato da IPZS o E	Segmento generato da MI
campi tabella [7.1-B]		campi 1-6 tabella [7.1-A]	campi 7-13 tabella [7.1-A]

Questi record contengono dunque richieste (di IPZS o E) ed approvazioni (di CA), e permettono di far avanzare la carta da uno stato di lavorazione all'altro, lungo il "percorso" che la porta dalla manifattura fino al momento del rilascio al titolare.

Questo flusso di richiesta ed approvazione è lo stesso utilizzato anche per il microcircuito, per cui nel record di controllo sono presenti elementi che andranno poi memorizzati nel chip (come il certificato C_Carta), e che consentono in tal modo anche un utile corrispondenza dei dati tra chip e banda ottica.

La tabella seguente definisce la struttura (campi) del record di controllo:

Campo	Generato da	Descrizione	Note
1	IPZS, E (S)	Numero progressivo del record nell'ambito della carta	sempre presente
2	IPZS, E (S)	Tipo del record (ossia dell'operazione)	Inizializzazione o Emissione
3	IPZS, E (S)	Data e ora della creazione del record	sempre presente
4	IPZS, E (S)	Certificato dell'ente che ha creato il record	Sempre presente. Emesso da CA.
5	IPZS, E (S)	Identificativo dell'operatore che ha creato il record	sempre presente
6	IPZS (Fc), E (S)	Bollo elettronico dell'ente che ha creato il record.	firma del record dati (Rd) e dei campi [1-5] del corrispondente record di controllo (Rc).
7	CA	Numero progressivo dell'autorizzazione concessa (generato secondo un protocollo interno di CA)	sempre presente.
8	CA	Data ed ora dell'autorizzazione	sempre presente
9	CA	Numero identificativo della carta	È il numero assegnato al documento d'identità da CA e presente anche sul supporto plastico
10	CA	Certificato della CA	sempre presente

11	CA	Identificativo dell'operatore che ha creato il record	Usualmente assente. presente solo su intervento manuale di un operatore nella generazione del record.
12	CA	Certificato anti-contraffazione della carta	E' il certificato rilasciato da CA che lega in modo biunivoco microprocessore e banda ottica.
13	CA	Bollo elettronico dell'ente di controllo e verifica	firma del record dati (Rd) e dei campi [1-12] del corrispondente record di controllo (Rc).
14	C.N.S.D.	Comune	Codice Belfiore del comune
15	C.N.S.D.	Provincia	Sigla della provincia

La seguente tabella definisce la struttura (campi) del record dati.

Campo	**Generato da**	**Descrizione**	**Note**
1	IPZS	E Numero progressivo del record nell'ambito dell'area dati (File_dati). Il numero progressivo di ogni record dell'area dati deve corrispondere a quello del record dell'area di controllo che descrive l'operazione eseguita per generarlo e contiene le relative approvazioni (firme)	sempre presente
2	E	Embedded Hologram	"impresso" anche in evidenza visiva sulla banda ottica al momento dell'emissione.
3	IPZS	Dati identificativi univoci della banda ottica (n. serie, lotto di	Non nullo nel record relativo all'inizializzazione, eseguita da IPZS.

		produzione, fabbricante, ecc.)	
4	E	Chiave biometrica individuale	Vuoto (opzionalmente valorizzato)
5	E	Dati riferiti alla persona, con l'eccezione della fotografia e della sottoscrizione del titolare.	Non nullo nel record relativo all'emissione
6	E	Fotografia	Non nullo nel record relativo all'emissione
7	E	Sottoscrizione del titolare	Non nullo nel record relativo all'emissione

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

7.2.2 Struttura delle informazioni nel microprocessore

La successiva tabella definisce la struttura di massima dei dati registrati nella memoria riscrivibile (EEPROM) del microcircuito.

Fornito da: indica l'operazione in ragione della quale viene messo a disposizione un contenuto informativo, consistente in una sequenza di *bytes*. Ad esempio, il risultato della raccolta dei dati riferiti alla persona del titolare, effettuata dall'ente emettitore (il Comune).

Predisposto da: indica l'operazione di creazione di una nuova struttura dati (DF o EF), ossia di un "contenitore" vuoto, pronto ad essere riempito con le informazioni che risultano da un'operazione del tipo precedente.

Scritto da: è l'operazione con la quale un contenitore vuoto (EF) viene riempito con le informazioni che risultano da una precedente operazione di generazione.

#	*Elemento*	*Fornito da*	*Predisposto da*	*Scritto da*	*Descrizione*
1	MF		IPZS		"Master File" del file system CIE.
2	DF0		IPZS		Dedicated file (directory).
3	DF1		IPZS		Dedicated file (directory).
4	DF2		IPZS		Dedicated file (directory).
5	PIN	E	E	E	PIN utente che abilita l'uso della chiave privata Kpri per le operazioni di autenticazione.
	PUK	E	E	E	PUK utente che abilita lo sblocco della carta nel caso non si disponga del PIN.

	PIN_SO		IPZS		PIN di Security Officer, abilita all'installazione della firma digitale.
6	Kpri		E		Chiave interna abilitabile in sola esecuzione e mai in lettura per operazioni crittografiche. invisibile all'esterno,
7	INSTpub EF_INST_FILE	E E	IPZS IPZS	IPZS IPZS	Chiave pubblica per installazione delle strutture dati relative ai servizi file elementare. contiene le chiavi per l'installazione dei servizi qualificati.
8	Dati_processore	IPZS	IPZS	IPZS	file elementare (EF)
9	Parametri_APDU	Fp	IPZS	IPZS	file elementare(EF).
10	ID_Carta	CA	IPZS	IPZS	Numero identificativo della carta d'identità. stampato da IPZS sul supporto.
11	C_Carta	CA	IPZS	E	certificato, rilasciato da CA contiene anche , l'hash sui dati identificativi.
12	Dati_personali	E	IPZS	E	file elementare che contiene i dati riferiti alla persona, con l'eccezione della fotografia.
13	Dati_personali aggiuntivi	E	IPZS	E	file elementare che contiene personali aggiuntivi.
14	Memoria_residua	E	IPZS	E	ammontare dello spazio totale previsto per i servizi, decurtato

					dello spazio utilizzato da quelli già installati.
15	Servizi_installati	E	IPZS	E	file elementare che riporta l'elenco dei servizi già installati sulla carta.
16	DF_Servizio #1, DF_Servizio #2, ... DF_Servizio #N	E	E	E	DF relativI ai servizi installati sulla carta.
17	DF_FIRMA		IPZS	E	DF relativo ai servizi di firma digitale.

Le presenti specifiche verranno aggiornate a cura del Comitato tecnico-scientifico permanente e pubblicate sul sito.

7.3 Le fasi preliminari

L'Istituto Poligrafico, responsabile della manifattura della CIE, riceve l'autorizzazione del Ministero dell'Economia e Finanze in merito alle richieste di fornitura di "documenti in bianco", distinte per Comune, avanzate in via telematica dalle Prefetture per il tramite del Ministero dell'Interno.
La consegna, alle Prefetture, dei "documenti in bianco" avviene al termine delle seguenti sottofasi di generazione numeri identificativi, produzione, inizializzazione ed incisione grafica degli elementi costanti.

7.3.1 Generazione numeri identificativi per le carte d'identità ed i documenti elettronici.

L'IPZS richiede alla CA i numeri identificativi (ID_Carta) necessari;

- La CA genera i nuovi ID_Carta ed inserisce un equivalente numero di record "in attesa"di divenire CIE nel suo database centrale;
- L'IPZS riceve via telematica i lotti di numeri identificativi da assegnare alle nuove carte in corso di produzione.

7.3.2 Produzione

L'IPZS, attiva le procedure necessarie ai fini della:

- predisposizione del supporto fisico;
- inserimento nel supporto fisico della pellicola di banda ottica e del microprocessore;
- stampa del logo e degli elementi grafici costanti e di sicurezza;
- inizializzazione elettrica del microprocessore.

7.3.3 Inizializzazione

La sottofase di inizializzazione, una delle più delicate dell'intero processo di emissione, consente di trasformare i tre supporti previsti, in un unico elemento inscindibile.

Dopo la fase di integrazione fisica del supporto plastico, con la banda ottica e il microprocessore, l'inizializzazione provvede alla integrazione logica tramite l'apposizione di codici univoci.

Mentre risulta di immediata applicazione il codice apposto sul supporto fisico l'inizializzazione di quelli informatici ha quale prerequisito la loro "formattazione" che, di fatto, consiste nella loro strutturazione in "directory" e l'impostazione delle condizioni di test necessarie a definire i diritti di accesso alle directory.
Le directory, definite in dettaglio nei precedenti paragrafi, servono per tracciare tutte le fasi di inizializzazione e personalizzazione della Carta, per consentire l'installazione dei servizi qualificati e per normalizzare i dati identificativi del titolare, le informazioni alfanumeriche, nonché le immagini.
In particolare l'IPZS provvede alla:

- generazione della struttura dati interna della banda ottica;
- generazione della struttura dati interna del microprocessore;
- scrittura dei files elementari che riportano i dati specifici del microprocessore ("Dati_processore"), della banda ottica ("Dati_banda_ottica") e del sistema operativo ("Parametri_APDU");
- scrittura ID_Carta;
- impostazione delle condizioni di accesso a tali file;
- scrittura del record dati (RD) e di alcuni campi (1-6) di quello di controllo (RC) relativi all'operazione di inizializzazione. Il record di controllo deve contenere almeno:
  - ID_Carta;

- Dati_Processore / Dati_Banda_Ottica;
- Data di fabbricazione;
- PIN P1 (per abilitare l'accesso in scrittura dei files elementari che devono essere riempiti dal Comune o dal CAPS al momento della formazione della carta) cifrato con la chiave pubblica del Comune o del CAPS di destinazione;
- Indicazione del Comune, dell'Ufficio Consolare o del CAPS cui la carta è destinata;

• inserimento del record dati e di quello di controllo in coda ad un file per il popolamento del Database del sistema di sicurezza del C.N.S.D., file che è inviato al C.N.S.D. per ottenere la approvazione delle carte prodotte;

• stoccaggio della carta.

7.3.4 Attivazione

Al termine della presente sottofase la carta d'identità risulta "attivata", e diventa "documento in bianco", ossia pronto alla fase successiva di formazione e rilascio, ad opera dei Comuni o dei CAPS.

Durante la presente sottofase l'IPZS esegue le seguenti attività:

- riceve dal Sistema di Sicurezza del C.N.S.D. il file di approvazione per distribuire il lotto di carte;
- consegna le carte in bianco attivate, i cui numeri di identificazione id_carta sono presenti nel file di approvazione ricevuto dal C.N.S.D., al magazzino del Tesoro del MEF. Il magazzino del Tesoro invia le carte in bianco attivate alle Prefetture , incaricati della distribuzione ai Comuni nella provincia di loro competenza, al MAE per la distribuzione agli Uffici Consolari, e ai CAPS.

Al completamento di questa fase il data base del Sistema di Sicurezza del C.N.S.D. conterrà tanti record quante sono le carte in bianco in attesa di formazione. Tali record contengono già informazioni come il numero identificativo della carta (ID_Carta), la Provincia ed il Comune di destinazione o l'Ufficio Consolare o il CAPS.

Durante la fase di personalizzazione, i campi di tali record verranno ulteriormente popolati con i codici fiscali (scritti in chiaro) dei titolari e con i dati identificativi (scritti in forma cifrata) degli stessi e per le carte assegnate ai CAPS, delle associazioni con Provincia e Comune.

La cifratura avverrà, tramite un sistema automatico, utilizzando la chiave pubblica della

Questura, territorialmente competente, e quella del Comune che ha rilasciato la Carta d'Identità Elettronica.

7.4 Personalizzazione ed emissione delle carte

La formazione delle carte ed il loro rilascio è condotta direttamente dai Comuni. In particolare, in base all'art. 13 (Procedura di sicurezza per la formazione e rilascio del documento) la fase di personalizzazione e stampa può essere svolta dai CAPA dei Comuni, dagli Uffici Consolari o dai CAPS gestiti dall'IPZS.
Nei paragrafi successivi le chiavi asimmetriche dei Comuni, degli Uffici Consolari, dei CAPA o dei CAPS saranno indicate con la seguente notazione:

- Kpri-aut, chiave privata di autenticazione, (per le comunicazioni protette con il C.N.S.D. gestite direttamente dal software di sicurezza fornito dal C.N.S.D.);
- Kpub-aut, chiave pubblica di autenticazione (per le comunicazioni protette con il C.N.S.D., gestite direttamente dal software di sicurezza fornito dal C.N.S.D.);
- Kpri-enc, chiave privata di crittografia (per cifrare i dati);
- Kpub-enc, chiave pubblica di crittografia (per cifrare i dati);
- Kpri-sig, chiave privata di bollo (per la firma dei dati);
- Kpub-sig, chiave pubblica bollo (per la firma dei dati).

7.4.1 Ricezione dei documenti in bianco (fa riferimento all'art. 12 del D.M.)

- Il Comune dotato di CAPA, il CAPA realizzato in forma associata o il CAPS riceve i documenti in bianco;
- I documenti devono essere conservati in appositi armadi di sicurezza, possibilmente in locali ad accesso riservato.

7.4.1.1 Sottofase di Compilazione

Questa sottofase, di front-office e che richiede la presenza dell'utente richiedente la CIE, viene svolta presso lo sportello comunale/Ufficio Consolare di front-office e consiste nell'acquisizione dei dati anagrafici e biometrici del richiedente.
In caso di comunicazione con l'anagrafe comunale la stessa deve avvenire in modalità diretta, senza creare archivi strutturati intermedi di dati anagrafici, anche se temporanei.

La procedura richiede anche la verifica della presenza in I.N.A. dell'utente richiedente. Nel caso l'utente non sia presente in I.N.A. il Comune provvede in autonomia all'inserimento, l'Ufficio Consolare lo richiede al Comune titolare dell'AIRE.
Il Comune/Ufficio Consolare genera, con modalità che rispettano i richiesti standard di sicurezza, i codici cifrati, necessari alla identificazione del documento.
Il Comune/Ufficio Consolare trasmette in via telematica al Sistema di Sicurezza del C.N.S.D. il messaggio informatico cifrato, costituito dai dati del richiedente e dai codici cifrati necessari all'identificazione del documento.
Tramite il software di sicurezza, le informazioni identificative del richiedente sono riportate, cifrate, dal Comune/Ufficio Consolare nel Sistema di Sicurezza del C.N.S.D..
I dati sono quelli indicati in dettaglio al paragrafo 4.4.
La fotografia può essere catturata direttamente, tramite videocamera digitale o digitalizzata per mezzo di uno scanner, in conformita' alle norme ICAO sui formati di memorizzazione dei dati biometrici: per questo motivo le fotografie devono attenersi strettamente alle indicazioni specificate sul sito.
Anche per digitalizzare la firma del titolare puo' essere utilizzato uno scanner oppure puo' essere catturata direttamente tramite tavoletta grafica.

Per l'impronta digitale, il Comune/Ufficio Consolare deve utilizzare un lettore di impronte digitali (live scan).
Per la conformità con i documenti di viaggio, il riferimento è costituito dalla Regulation (EC) 2257/2004 e succ. aggiornamenti e dalle già richiamate norme ICAO 9303.

Cifratura simmetrica dei dati almeno a 128 bit. La cifratura viene eseguita automaticamente dal software di sicurezza. La cifratura e' indispensabile per proteggere i dati durante la trasmissione al Sistema di Sicurezza del C.N.S.D. utilizzando la Kpub-enc del Sistema di Sicurezza del C.N.S.D. stesso con una chiave di trasporto almeno da 128 bit generata in maniera dinamica sessione per sessione SSL V3 strong attivato mediante utilizzo delle chiavi Kpub-aut e Kpri-aut del Comune/Ufficio Consolare.
Apposizione del bollo elettronico del Comune/Ufficio Consolare, per mezzo della Kpri-sig (Comune/Ufficio Consolare). L'apposizione di tale bollo garantisce il mittente al Sistema di Sicurezza del C.N.S.D..
Invio delle richieste di emissione carta d'identita', anche strutturate in lotti, al Sistema di Sicurezza del C.N.S.D. per via telematica.

Le seguenti attività sono svolte presso il C.N.S.D., in risposta all'invio da parte del Comune/Ufficio Consolare, dei dati raccolti dal front-office, anche strutturati in lotti.

Il Sistema di sicurezza del C.N.S.D.:

1) riceve i dati raccolti dal front-office del Comune/Ufficio Consolare;
2) estrae, tramite la la propria Kpri-enc, i record dati;
3) mantiene in chiaro codice fiscale, provincia e comune/Ufficio Consolare richiedente e cifra per il cartellino elettronico tutte le altre informazioni con due chiavi: la Kpub-enc del Comune/Ufficio Consolare richiedente e la Kpub-enc della Questura territorialmente competente;
4) per ogni richiesta, esegue il controllo automatico di "non esistenza" sulla propria base dati, tramite i dati in chiaro;
   1) Controllo positivo (es. CIE già rilasciata per quel codice fiscale, richiesta avanzata da un Comune/Ufficio Consolare diverso da quello previsto, etc.) viene rigettata la richiesta non vengono seguite ulteriori attività e al Comune/Ufficio Consolare viene ritornato un opportuno codice di errore.
   2) Controllo negativo (la richiesta può essere soddisfatta).

7.4.1.2 Sottofase di autorizzazione

La sottofase di autorizzazione**,** fase di back-office svolta presso il C.N.S.D.**,** viene effettuata dal Sistema di Sicurezza del C.N.S.D. successivamente al controllo negativo (7.4.1.1 comma 4.2) di richieste di emissione provenienti dai Comuni.

Tutte le comunicazioni, gestite dal software di sicurezza del C.N.S.D., utilizzano cifratura simmetrica dei dati almeno a 128 bit. La cifratura viene eseguita automaticamente dal software di sicurezza. La cifratura e' indispensabile per proteggere i dati durante gli scambi informativi con il Sistema di Sicurezza del C.N.S.D. utilizzando la Kpub-enc del Sistema di Sicurezza del C.N.S.D. stesso con una chiave di trasporto almeno da 128 bit generata in maniera dinamica sessione per sessione SSL V3 strong attivato mediante utilizzo delle chiavi Kpub-aut e Kpri-aut del CAPA o del CAPS;
Apposizione del bollo elettronico, per mezzo della Kpri-sig (CAPA, CAPS).

Il Sistema di sicurezza del C.N.S.D., per le carte che devono essere allestite presso i Comuni, o Uffici Consolari, dotati di CAPA:

1) riceve le richieste di firma dei certificati da memorizzare sulle CIE, formate presso i Comuni o Uffici Consolari dotati di CAPA a partire dalla generazione a bordo dei microprocessori delle CIE delle chiavi asimmetriche;

2) genera i certificati digitali firmati dalla CA del C.N.S.D.
3) completa la scrittura dei cartellini elettronici e la loro archiviazione presso il C.N.S.D. per i Comuni e le Questure territorialmente competenti;
4) invia i certificati generati ai Comuni, o Uffici Consolari, dotati di CAPA, per l'allestimento e stampa delle CIE corrispondenti.

Il Sistema di sicurezza del C.N.S.D., per le carte che devono essere allestite presso i CAPS:

1) raccoglie le richieste di emissione CIE provenienti dai Comuni e, a cadenze temporali prefissate, predispone un elenco di richieste di allestimento e stampa di CIE, classificato per Comune/Ufficio Consolare e lo invia telematicamente in sicurezza al CAPS;
2) riceve in sicurezza dal CAPS il corrispondente elenco contenente le richieste di firma dei certificati da memorizzare sulle CIE, formate presso il CAPS a partire dalla generazione a bordo dei microprocessori delle CIE delle chiavi asimmetriche;
3) genera i certificati digitali firmati dalla CA del C.N.S.D.;
4) completa la scrittura dei cartellini elettronici e la loro archiviazione presso il C.N.S.D. per i Comuni e le Questure territorialmente competenti;
5) a cadenze temporali prefissate, invia in sicurezza al CAPS l'elenco contenente i certificati generati e i dati necessari per l'allestimento e stampa delle CIE corrispondenti.

7.4.1.3 Sottofase di formazione

Sottofase di back-office di competenza dell'Ente incaricato dell'allestimento della CIE (Comune, o Ufficio Consolare, dotato di CAPA, o CAPS) che riporta i dati su tutti i supporti: microprocessore, banda ottica e grafici sul supporto fisico. La criticità maggiore sta nel fatto che, qualsiasi inconveniente possa verificarsi non deve mettere a rischio l'integrità dei dati (per es. scrivendo infomazioni diverse sui vari supporti). Allo scopo si suggerisce di garantire agli strumenti informatici continuità elettrica.

1) Il Comune, o Ufficio Consolare, dotato di CAPA, o il CAPS:
   a. riceve il record dati validato dalla CA del C.N.S.D.;
   b. memorizza i dati nel microprocessore;
   c. memorizza i dati nella banda ottica. Al fine di consentire una identificazione sicura, e dare certezza sulla originalità della CIE, i dati memorizzati nella banda ottica devono essere quelli firmati con il bollo elettronico del Sistema di Sicurezza del C.N.S.D..

d. stampa grafica dei dati sul supporto fisico.
e. nel caso del CAPS stampa con tecnologia “Laser Engraving” sul supporto fisico il nome del Comune di destinazione.
f. Comunica al C.N.S.D. l’esito dell’operazione di formazione delle CIE che lo rende disponibile al Comune.

7.4.1.4 Sottofase di rilascio

Questa sottofase, di front-office e svolta in presenza dell’utente, e’ di esclusiva competenza dei Comuni che:

1) stampano il PIN utente su speciale carta chimica retinata, tale da garantire la riservatezza dell’informazione contenuta e di evidenziare eventuali tentativi di apertura.
2) rilasciano la CIE al cittadino che ne ha fatto richiesta verificando la correttezza dei dati identificativi del titolare;
3) consegnano la busta contenente il PIN utente;
4) comunicano al C.N.S.D. l’avvenuto rilascio tramite comunicazione telematica diretta.

Il C.N.S.D. notifica periodicamente all’Istituto l’elenco delle CIE rilasciate, per alimentare il sistema di contabilizzazione del MEF.

7.4.1.5 Sottofase di verifica e controllo

La verifica ed il controllo sono le uniche attività sempre presenti in tutte le sottofasi di lavorazione della CIE, dal momento della produzione fino al loro rilascio e vengono condotte dal Sistema di sicurezza del C.N.S.D.. Per questo motivo tutti gli enti coinvolti nei vari momenti del processo devono disporre di una connessione telematica con il C.N.S.D..

Ovviamente la verifica ed il controllo citato nel processo di formazione, non è riferito a quello che verrà dettagliato nel capitolo successivo che, invece, si riferisce ai controlli effettuabili dalla Polizia come previsto dal Testo Unico delle Leggi di P.S.

8 Verifica delle carte di identità elettroniche (fa riferimento all'art. 6, comma 1 del D.M.)

Nel presente capitolo sono descritti in dettaglio i casi in cui è consentito l'accesso alle CIE ed alle informazioni in esse contenute. Vengono, altresì, indicati gli organi competenti e le modalità di accesso.

8.1 Conservazione del cartellino elettronico (fa riferimento all'art. 6, comma 3 del D.M.)

Il processo di ammodernamento della CIE deve necessariamente portare ad una differente interpretazione di alcune delle norme precedenti, soprattutto di quelle destinate alla gestione del modello cartaceo, ormai superato.
E' pressoché intuitivo come non trovino ragione di essere le prescrizioni relative alla conservazione e consultazione della copia del cartellino presente in ciascuna Questura. L'obbligo previsto per i Comuni di trasmettere copia del cartellino per ogni carta di identità rilasciata, viene sostituito dalla seguente procedura prevista per il nuovo cartellino elettronico:

- i Comuni eseguono le attività di formazione e rilascio delle CIE;
- il Sistema di sicurezza del C.N.S.D. riceve comunicazione che è stata rilasciata la CIE e memorizza la copia elettronica, della stessa, nell'archivio di pertinenza della Questura territorialmente competente. La copia elettronica, viene cifrata con la chiave pubblica della Questura stessa. Tale modalità consente di attendere al Testo Unico delle Leggi di P.S. che indica nelle Questura l'ufficio a cui è demandata la conservazione della copia delle CIE;
- i controlli sulle CIE, una volta memorizzate, possono essere effettuati secondo le seguenti modalità:
  - da qualsiasi operatore delle Forze di Polizia tramite controlli a vista, apparecchiature standalone o transazioni a Sistema di Sicurezza del C.N.S.D.. In quest'ultimo caso, se la richiesta arriva da una Questura di una Provincia diversa da quella dove è stato rilasciata la CIE, l'operatore può, tramite il codice fiscale del titolare o il numero della CIE verificarne l'esistenza, il Comune e la provincia in cui è stata rilasciata, non può vedere nel dettaglio le informazioni della CIE;
  - da un operatore della Questura nella cui Provincia è stata rilasciata la CIE. In questo caso l'operatore può, tramite il codice fiscale del titolare o il numero di CIE, verificarne l'esistenza e, tramite l'inserimento della propria chiave privata, verificarne anche il contenuto nel dettaglio.
  - le Questure territorialmente competenti tramite Sistema di Sicurezza del C.N.S.D.

conservano e consultano la copia elettronica della CIE. Possono eseguire anche stampe e tutte le attività già possibili con la passata gestione.

8.2 Interdizione dell'operatività della CIE (fa riferimento all'art. 6, comma 2 del D.M.)

Le caratteristiche principali della nuova CIE, che la differenziano dal vecchio modello cartaceo, sono rappresentate dalla presenza dei supporti informatici e dalla gestione centralizzata del flusso di emissione. Entrambi gli elementi da un lato aumentano il livello di sicurezza del nuovo documento e dall'altro offrono la possibilità di accesso a servizi telematici sia nazionali che locali.

Proprio questa nuova possibilità di accedere a servizi implica la necessità di dover sospendere o interdire, più che in passato, l'utilizzo della CIE che potrebbe essere impiegata, in caso di furto o smarrimento, da persone diverse dal titolare.

Nel seguito vengono descritte le modalità a cui è necessario attenersi in caso di furto o smarrimento di una CIE.

- il titolare telefona al numero verde che trova pubblicato sul sito e segnala l'avvenuto smarrimento/furto della CIE, fornendo, con modalità automatiche, informazioni che consentano di identificarlo;
    - o la segnalazione del titolare e le informazioni relative alla sua identificazione, cifrate, sono memorizzate negli archivi di sicurezza del C.N.S.D.. La CIE segnalata dal titolare viene sospesa nei sistemi di sicurezza del C.N.S.D. che inviano la segnalazione di sospensione della CIE a tutti i punti di verifica di validità della CIE;
        - ▪ a partire dalla ricezione della segnalazione di sospensione della CIE, i sistemi di sicurezza del C.N.S.D. e i punti di accesso per le richieste di verifica di validità delle CIE forniscono risposta negativa alle richieste relative alla CIE segnalata;
- successivamente alla comunicazione telefonica, il titolare della CIE deve presentare regolare denuncia alle Forze dell'ordine, anche al fine di poter ottenere una nuova CIE dal Comune. Le Forze dell'ordine, attraverso i servizi di sicurezza del C.N.S.D. provvedono a segnalare al C.N.S.D. la sospensione della CIE nel caso in cui il

cittadino non ne avesse già richiesto la sospensione tramite telefonata al numero verde della CIE, e comunicano l'avvenuta regolare denuncia alla questura che provvede a interdire l'operatività della CIE;

- è compito della Questura, tramite i servizi di sicurezza del C.N.S.D., revocare l'interdizione dell'operatività della CIE, collegandosi ai servizi di sicurezza del C.N.S.D., quando il cittadino sia tornato in possesso della CIE e lo attesti presentando regolare denuncia. Lo stato della CIE è quindi ripristinato allo stato normale nei sistemi di sicurezza del C.N.S.D. che inviano i dati identificativi (id carta, dati identificativi del certificato digitale) della CIE non più interdetta a tutti i punti di verifica di validità delle CIE;
    - a partire dalla ricezione della segnalazione di ripristino dello stato della CIE, i sistemi di sicurezza del C.N.S.D. e i punti di accesso forniscono risposta positiva alle richieste di verifica di validità della CIE ripristinata;
- se il cittadino ottiene il rilascio di una nuova CIE, la vecchia CIE interdetta è revocata.

8.4. Procedure per l'installazione della firma digitale.

Per l'installazione del servizio qualificato di firma digitale, le procedure sono rese disponibili sul sito del Ministero dell'Interno, coerentemente con quanto stabilito al punto 6 e in conformità alla normativa vigente.

Per quanto concerne le CIE gia' circolanti, il servizio di firma digitale può essere installato, anche a cura dei Comuni, attenendosi alle specifiche regole tecniche di sicurezza, emanate dal Comitato di cui all'art 8-ter e pubblicate sul sito.

8.4.1 Certificati di firma digitale.

In accordo con quanto previsto dalla normativa vigente, il certificato di firma digitale per un utilizzo della CIE come strumento di sottoscrizione dei documenti, deve essere conforme alla normativa vigente anche in materia di interoperabilita'.

8.5 Impronte digitali.

Nella memoria del microchip della CIE *possono essere* installati i template numerici delle impronte digitali del titolare della carta. Il template è una rappresentazione numerica di un elemento biometrico (in questo caso l'impronta di due dita) e viene utilizzato ai fini di riconoscimento dell'impronta originale pur non consentendone una sua qualsivoglia ricostruzione. Tale riconoscimento non presuppone la presenza di nessuna banca dati

avvenendo il confronto direttamente tra il template memorizzato sulla CIE e quello generato durante la fase di lettura da parte dello specifico reader utilizzato dalla postazione client o sul server. Un simile confronto garantisce, per i servizi che lo richiedono, la presenza fisica del titolare della CIE.
Al fine di evitare qualsivoglia possibilità di manipolazione successiva, lo spazio dedicato alla memorizzazione del template, dopo la sua installazione, viene reso non riscrivibile. Più in dettaglio, durante la fase di installazione, le impronte assunte tramite lettori sono trasformate in template secondo lo specifico algoritmo fornito dal Ministero dell'Interno e memorizzate nell'area dedicata assieme ad un progressivo che può variare da zero a nove in funzione delle dita utilizzate per l'assunzione dell'impronta. Anche la fase di installazione delle impronte non comporta la memorizzazione di dati sulle postazioni dei Comuni emettitori.
Le impronte digitali e i relativi template restano quindi utilizzabili solo per la finalità di verifica dell'identità del titolare del documento e non sono in ogni caso registrati in banche di dati.

9. Livelli di servizio

I livelli di servizio offerti dalle infrastrutture tecnologiche descritte nel presente allegato sono aggiornati dal Comitato di indirizzo di cui all'art. 8-ter, a partire dai livelli indicati nel presente paragrafo, e pubblicati sul sito. Devono comunque essere presenti specifici livelli di servizio inerenti:

a) la disponibilità dei servizi applicativi offerti dalle infrastrutture tecnologiche:
   1. reti di accesso
   2. infrastruttura tecnologica
b) la disponibilità e i tempi di risposta del call center;

In particolare si assume che i livelli di servizio offerti per il servizio di call center siano almeno i seguenti:

Parametro da rilevare	Condizioni contrattuali	Limite	Base temporale di riferimento
Percentuale di chiamate entranti con risposta	--	99%	Mensile
Tempo di attesa delle chiamate	≤ 20 secondi nel 95% dei casi		Mensile
Tempo di risposta a richieste e-mail	≤ 1 ora nel 95% dei casi		Mensile
Tempo di risposta a richieste via fax	≤ 1 ora nel 95% dei casi		Mensile
Tempi di ripristino del disservizio di call center	≤ 8h nel 90% dei casi		Mensile

c) Servizi di firma digitale.
d) l'adeguatezza della documentazione presente sul sito e il suo aggiornamento.
e) Servizi di sicurezza del CNSD;

In particolare si assume che i livelli di servizio offerti dai servizi di sicurezza, di emissione CIE e di uso CIE del C.N.S.D., con particolare riferimento ai servizi di cui all'articolo 6.1, devono essere almeno i seguenti:

a) Servizi di emissione
   - a.1) a partire dal momento in cui un Comune richiede ai servizi di sicurezza del C.N.S.D. l'autorizzazione alla stampa del PIN, PUK e CIP di una CIE per la quale sia stata già richiesta ai servizi del C.N.S.D. da parte del Comune stesso o di un CAPS l'autorizzazione all'allestimento e il conseguente rilascio del certificato da parte della certification authority del C.N.S.D., il C.N.S.D., entro sessanta secondi, deve iniziare l'attivazione dei collegamenti di rete con tutti i punti di accesso e, per ogni punto trovato attivo, deve inviare gli identificativi necessari e sufficienti a fornire risposta positiva per tutte le richieste di verifica di validità che da questo momento in poi potranno essere presentate per la CIE in fase di emissione.
     - a.1.i) se un punto di accesso non viene trovato attivo per tre volte in un giorno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.
     - a.1.ii) se un punto di accesso non viene trovato attivo per più di sei volte in un mese o per più di trenta volte in un anno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

b) Servizi di verifica della validità della CIE rispetto alla sua qualità di documento di riconoscimento dell'identità personale: servizi di sospensione e di ripristino da interdizione
   - b.1) a partire dal momento in cui i servizi di sicurezza del C.N.S.D. ricevono una segnalazione di sospensione di una CIE, il C.N.S.D., entro sessanta secondi, deve iniziare l'attivazione dei collegamenti di rete con tutti i punti di accesso e, per ogni

punto trovato attivo, deve inviare gli identificativi necessari e sufficienti a fornire risposta negativa per le richieste di verifica di validità CIE che perverranno dal momento di invio della segnalazione.

b.1.i) se un punto di accesso non viene trovato attivo per tre volte in un giorno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

b.1.ii) se un punto di accesso non viene trovato attivo per più di sei volte in un mese o per più di trenta volte in un anno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

b.2) a partire dal momento in cui i servizi di sicurezza del C.N.S.D. ricevono una segnalazione di cancellazione dell'interdizione di una CIE, il C.N.S.D., entro sessanta secondi, deve iniziare l'attivazione dei collegamenti di rete con tutti i punti di accesso e, per ogni punto trovato attivo, deve inviare gli identificativi necessari e sufficienti a fornire risposta positiva per le richieste di verifica di validità della CIE segnalata.

b.2.i) se un punto di accesso non viene trovato attivo per tre volte in un giorno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

b.2.ii) se un punto di accesso non viene trovato attivo per più di sei volte in un mese o per più di trenta volte in un anno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

c) - Servizi di uso della CIE

c.1) a partire dal momento in cui un punto di accesso riceve dal C.N.S.D. una segnalazione su una CIE con le informazioni necessarie e sufficienti di cui ai precedenti punti a.1), b.1) e b.2) il punto di accesso entro 120 secondi deve essere in grado di fornire risposte corrette relativamente alla CIE segnalata:

c.1.i) se un punto di accesso non rispetta il termine dei 120 secondi per più di tre volte in un giorno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

c.1.ii) se un punto di accesso non rispetta il termine dei 120 secondi per più di sei volte in un mese o per più di trenta volte in un anno, il sistema di sicurezza del C.N.S.D. provvede a disabilitare il punto di accesso stesso, revocandone il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

c.2) Servizi OCSP di verifica dei certificati digitali delle CIE: i servizi di OCSP relativi alla sospensione e/o revoca della validità del certificato digitale della CIE hanno i seguenti livelli di servizio:

Parametro da rilevare	**Condizioni contrattuali**	**Limite**	**Base temporale di riferimento**
Disponibilità del sistema di validazione on line	7/7*24h e conforme con le specifiche tecniche OCSP (RFC 2560)	99%	Mensile
Durata delle interruzioni del sistema di validazione on line	2 ore	99%	Mensile
Tempo di risposta del sistema di validazione on line	5 sec nel 90% dei casi		Settimanale

Gli ulteriori i livelli di servizio richiesti ai punti di accesso sono i seguenti:

- disponibilità del servizio >= 99.9% (esclusi i downtime programmati)
- funzionamento h24, 7 giorni su 7.

In caso di non soddisfazione dei livelli di servizio da parte di un punto di accesso, il punto di accesso è disabilitato e i sistemi di sicurezza del C.N.S.D. ne revocano il certificato digitale emesso dalla certification authority del C.N.S.D. che consente al punto di accesso stesso di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

I sistemi di sicurezza del C.N.S.D. provvedono ad emettere i certificati di firma che abilitano i punti di accesso consentendogli di autenticare le loro risposte alle richieste di verifica di validità CIE provenienti dal territorio.

Al fine di misurare i livelli di servizio, i servizi di sicurezza del C.N.S.D. utilizzano agenti software di monitoraggio e misura dei livelli di servizio che devono essere installati presso tutti i punti dove è richiesta la misura dei livelli di servizio.
L'assenza o il non funzionamento dell'agente software di monitoraggio e misura dei livelli di servizio presso un punto di accesso portano alla revoca automatica ed immediata del certificato digitale che abilita il punto di accesso consentendogli di autenticare le sue risposte alle richieste di verifica di validità CIE provenienti dal territorio.

L'attivazione dei livelli di servizio sarà regolata da un decreto del Ministro dell'Interno.

Il Comitato di indirizzo e monitoraggio fornirà gli ulteriori livelli di servizio relativi alle attività dell'Istituto.

07A09524

AUGUSTA IANNINI, *direttore* GABRIELE IUZZOLINO, *redattore*

(G703217/1) Roma, 2007 - Istituto Poligrafico e Zecca dello Stato S.p.A. - S.

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE

cap	località	libreria	indirizzo	pref.	tel.	fax
00041	**ALBANO LAZIALE (RM)**	LIBRERIA CARACUZZO	Corso Matteotti, 201	06	9320073	93260286
60121	**ANCONA**	LIBRERIA FOGOLA	Piazza Cavour, 4-5-6	071	2074606	2060205
81031	**AVERSA (CE)**	LIBRERIA CLA.ROS	Via L. Da Vinci, 18	081	8902431	8902431
70124	**BARI**	CARTOLIBRERIA QUINTILIANO	Via Arcidiacono Giovanni, 9	080	5042665	5610818
70121	**BARI**	LIBRERIA EGAFNET.IT	Via Crisanzio, 16	080	5212142	5243613
13900	**BIELLA**	LIBRERIA GIOVANNACCI	Via Italia, 14	015	2522313	34983
40132	**BOLOGNA**	LIBRERIA GIURIDICA EDINFORM	Via Ercole Nani, 2/A	051	4218740	4210565
40124	**BOLOGNA**	LIBRERIA GIURIDICA - LE NOVITÀ DEL DIRITTO	Via delle Tovaglie, 35/A	051	3399048	3394340
21052	**BUSTO ARSIZIO (VA)**	CARTOLIBRERIA CENTRALE BORAGNO	Via Milano, 4	0331	626752	626752
91022	**CASTELVETRANO (TP)**	CARTOLIBRERIA MAROTTA & CALIA	Via Q. Sella, 106/108	0924	45714	45714
95128	**CATANIA**	CARTOLIBRERIA LEGISLATIVA S.G.C. ESSEGICI	Via F. Riso, 56/60	095	430590	508529
88100	**CATANZARO**	LIBRERIA NISTICÒ	Via A. Daniele, 27	0961	725811	725811
66100	**CHIETI**	LIBRERIA PIROLA MAGGIOLI	Via Asinio Herio, 21	0871	330261	322070
22100	**COMO**	LIBRERIA GIURIDICA BERNASCONI - DECA	Via Mentana, 15	031	262324	262324
87100	**COSENZA**	LIBRERIA DOMUS	Via Monte Santo, 70/A	0984	23110	23110
50129	**FIRENZE**	LIBRERIA PIROLA già ETRURIA	Via Cavour 44-46/R	055	2396320	288909
71100	**FOGGIA**	LIBRERIA PATIERNO	Via Dante, 21	0881	722064	722064
16121	**GENOVA**	LIBRERIA GIURIDICA	Galleria E. Martino, 9	010	565178	5705693
95014	**GIARRE (CT)**	LIBRERIA LA SEÑORITA	Via Trieste angolo Corso Europa	095	7799877	7799877
73100	**LECCE**	LIBRERIA LECCE SPAZIO VIVO	Via Palmieri, 30	0832	241131	303057
74015	**MARTINA FRANCA (TA)**	TUTTOUFFICIO	Via C. Battisti, 14/20	080	4839784	4839785
98122	**MESSINA**	LIBRERIA PIROLA MESSINA	Corso Cavour, 55	090	710487	662174
20100	**MILANO**	LIBRERIA CONCESSIONARIA I.P.Z.S.	Galleria Vitt. Emanuele II, 11/15	02	865236	863684

Segue: **LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE**

cap	località	libreria	indirizzo	pref.	tel.	fax
80134	**NAPOLI**	LIBRERIA LEGISLATIVA MAJOLO	Via Tommaso Caravita, 30	081	5800765	5521954
28100	**NOVARA**	EDIZIONI PIROLA E MODULISTICA	Via Costa, 32/34	0321	626764	626764
90138	**PALERMO**	LA LIBRERIA DEL TRIBUNALE	P.za V.E. Orlando, 44/45	091	6118225	552172
90138	**PALERMO**	LIBRERIA S.F. FLACCOVIO	Piazza E. Orlando, 15/19	091	334323	6112750
90145	**PALERMO**	LA LIBRERIA COMMISSIONARIA	Via S. Gregorietti, 6	091	6859904	6859904
90133	**PALERMO**	LIBRERIA FORENSE	Via Maqueda, 185	091	6168475	6177342
43100	**PARMA**	LIBRERIA MAIOLI	Via Farini, 34/D	0521	286226	284922
06087	**PERUGIA**	CALZETTI & MARIUCCI	Via della Valtiera, 229	075	5997736	5990120
29100	**PIACENZA**	NUOVA TIPOGRAFIA DEL MAINO	Via Quattro Novembre, 160	0523	452342	461203
59100	**PRATO**	LIBRERIA CARTOLERIA GORI	Via Ricasoli, 26	0574	22061	610353
00192	**ROMA**	LIBRERIA DE MIRANDA	Viale G. Cesare, 51/E/F/G	06	3213303	3216695
00187	**ROMA**	LIBRERIA GODEL	Via Poli, 46	06	6798716	6790331
00187	**ROMA**	STAMPERIA REALE DI ROMA	Via Due Macelli, 12	06	6793268	69940034
63039	**SAN BENEDETTO D/T (AP)**	LIBRERIA LA BIBLIOFILA	Via Ugo Bassi, 38	0735	587513	576134
10122	**TORINO**	LIBRERIA GIURIDICA	Via S. Agostino, 8	011	4367076	4367076
36100	**VICENZA**	LIBRERIA GALLA 1880	Viale Roma, 14	0444	225225	225238

MODALITÀ PER LA VENDITA

La «Gazzetta Ufficiale» e tutte le altre pubblicazioni dell'Istituto sono in vendita al pubblico:

- **— presso l'Agenzia dell'Istituto Poligrafico e Zecca dello Stato S.p.A. in ROMA, piazza G. Verdi, 10 - ☎ 06 85082147;**
- **— presso le librerie concessionarie indicate (elenco consultabile sul sito www.ipzs.it)**

L'Istituto conserva per la vendita le Gazzette degli ultimi 4 anni fino ad esaurimento. Le richieste per corrispondenza potranno essere inviate a:

Funzione Editoria - U.O. DISTRIBUZIONE
Attività Librerie concessionarie, Vendita diretta e Abbonamenti a periodici
Piazza Verdi 10, 00198 Roma
fax: 06-8508-4117
e-mail: editoriale@ipzs.it

avendo cura di specificare nell'ordine, oltre al fascicolo di GU richiesto, l'indirizzo di spedizione e di fatturazione (se diverso) ed indicando il codice fiscale per i privati. L'importo della fornitura, maggiorato di un contributo per le spese di spedizione, sarà versato in contanti alla ricezione.

Le inserzioni, come da norme riportate nella testata della parte seconda, si ricevono con pagamento anticipato, presso le agenzie in Roma e presso le librerie concessionarie.

Per informazioni, prenotazioni o reclami attinenti agli abbonamenti oppure alla vendita della *Gazzetta Ufficiale* bisogna rivolgersi direttamente all'Amministrazione, presso l'Istituto Poligrafico e Zecca dello Stato - Piazza G. Verdi, 10 - 00100 ROMA

Gazzetta Ufficiale Abbonamenti	Vendite	Ufficio inserzioni	Numero verde
☎ 800-864035 - Fax 06-85082520	☎ 800-864035 - Fax 06-85084117	☎ 800-864035 - Fax 06-85082242	☎ 800-864035

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

CANONI DI ABBONAMENTO ANNO 2008 (salvo conguaglio) (*)

GAZZETTA UFFICIALE - PARTE I (legislativa)

			CANONE DI ABBONAMENTO
Tipo A	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari:		
	(di cui spese di spedizione € 257,04)	- annuale	€ **438,00**
	(di cui spese di spedizione € 128,52)	- semestrale	€ **239,00**
Tipo A1	Abbonamento ai fascicoli della serie generale, inclusi i soli supplementi ordinari contenenti i provvedimenti legislativi:		
	(di cui spese di spedizione € 132,57)	- annuale	€ **309,00**
	(di cui spese di spedizione € 66,28)	- semestrale	€ **167,00**
Tipo B	Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte Costituzionale:		
	(di cui spese di spedizione € 19,29)	- annuale	€ **68,00**
	(di cui spese di spedizione € 9,64)	- semestrale	€ **43,00**
Tipo C	Abbonamento ai fascicoli della serie speciale destinata agli atti della CE:		
	(di cui spese di spedizione € 41,27)	- annuale	€ **168,00**
	(di cui spese di spedizione € 20,63)	- semestrale	€ **91,00**
Tipo D	Abbonamento ai fascicoli della serie destinata alle leggi e regolamenti regionali:		
	(di cui spese di spedizione € 15,31)	- annuale	€ **65,00**
	(di cui spese di spedizione € 7,65)	- semestrale	€ **40,00**
Tipo E	Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:		
	(di cui spese di spedizione € 50,02)	- annuale	€ **167,00**
	(di cui spese di spedizione € 25,01)	- semestrale	€ **90,00**
Tipo F	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari, ed ai fascicoli delle quattro serie speciali:		
	(di cui spese di spedizione € 383,93)	- annuale	€ **819,00**
	(di cui spese di spedizione € 191,46)	- semestrale	€ **431,00**
Tipo F1	Abbonamento ai fascicoli della serie generale inclusi i supplementi ordinari con i provvedimenti legislativi e ai fascicoli delle quattro serie speciali:		
	(di cui spese di spedizione € 264,45)	- annuale	€ **682,00**
	(di cui spese di spedizione € 132,22)	- semestrale	€ **357,00**

N.B.: L'abbonamento alla GURI tipo A, A1, F, F1 comprende gli indici mensili
Integrando con la somma di € 80,00 il versamento relativo al tipo di abbonamento alla *Gazzetta Ufficiale* - parte prima - prescelto, si riceverà anche l'**Indice Repertorio Annuale Cronologico per materie anno 2008.**

CONTO RIASSUNTIVO DEL TESORO

Abbonamento annuo (incluse spese di spedizione) € **56,00**

PREZZI DI VENDITA A FASCICOLI
(Oltre le spese di spedizione)

Prezzi di vendita:		
	serie generale	€ 1,00
	serie speciali (escluso concorsi), ogni 16 pagine o frazione	€ 1,00
	fascicolo serie speciale, *concorsi,* prezzo unico	€ 1,50
	supplementi (ordinari e straordinari), ogni 16 pagine o frazione	€ 1,00
	fascicolo Bollettino Estrazioni, ogni 16 pagine o frazione	€ 1,00
	fascicolo Conto Riassuntivo del Tesoro, prezzo unico	€ 6,00

I.V.A. 4% a carico dell'Editore

5ª SERIE SPECIALE - CONTRATTI ED APPALTI

(di cui spese di spedizione € 127,00)	- annuale	€ **295,00**
(di cui spese di spedizione € 73,00)	- semestrale	€ **162,00**

GAZZETTA UFFICIALE - PARTE II

(di cui spese di spedizione € 39,40)	- annuale	€ **85,00**
(di cui spese di spedizione € 20,60)	- semestrale	€ **53,00**

Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione (oltre le spese di spedizione) € 1,00
I.V.A. 20% inclusa

RACCOLTA UFFICIALE DEGLI ATTI NORMATIVI

Abbonamento annuo € **190,00**
Abbonamento annuo per regioni, province e comuni - SCONTO 5% € **180,50**
Volume separato (oltre le spese di spedizione) € 18,00
I.V.A. 4% a carico dell'Editore

Per l'estero i prezzi di vendita, in abbonamento ed a fascicoli separati, anche per le annate arretrate, compresi i fascicoli dei supplementi ordinari e straordinari, devono intendersi raddoppiati. Per il territorio nazionale i prezzi di vendita dei fascicoli separati, compresi i supplementi ordinari e straordinari, relativi ad anni precedenti, devono intendersi raddoppiati. Per intere annate è raddoppiato il prezzo dell'abbonamento in corso. Le spese di spedizione relative alle richieste di invio per corrispondenza di singoli fascicoli, vengono stabilite, di volta in volta, in base alle copie richieste.

N.B. - Gli abbonamenti annui decorrono dal 1° gennaio al 31 dicembre, i semestrali dal 1° gennaio al 30 giugno e dal 1° luglio al 31 dicembre.

RESTANO CONFERMATI GLI SCONTI IN USO APPLICATI AI SOLI COSTI DI ABBONAMENTO

ABBONAMENTI UFFICI STATALI
Resta confermata la riduzione del 52% applicata sul solo costo di abbonamento

* tariffe postali di cui al Decreto 13 novembre 2002 (G.U. n. 289/2002) e D.P.C.M. 27 novembre 2002 n. 294 (G.U. 1/2003) per soggetti iscritti al R.O.C.